

Annual Report – 2025

# Vulnerability Intelligence

Powered by  
**LOVI** 

login:soft

# Table of Contents

**Executive Summary: Cybersecurity Landscape in 2025** ..... 3

**Ransomware Activity in 2025** ..... 4

**New Ransomware Observed in 2025**..... 5

**Ransomware Insights – 2025**..... 7

**Most Observed Vulnerabilities from our Sensors** ..... 15

**Opensource Software Vulnerabilities abused by Threat Actors** ..... 16

**CISA Industrial Control Systems (ICS) General CVE's abused by Malware**..... 17

**Threat Activity Landscape in 2025** ..... 19

**Tracking CISA KEV – 2025** ..... 21

**Vendor-wise contributions to the CISA KEV Catalog** ..... 22

**Monthly Breakdown of Actively Exploited Vulnerabilities** ..... 24

**January** ..... 24

**February** ..... 27

**March** ..... 29

**April**..... 32

**May**..... 35

**June** ..... 37

**July** ..... 39

**August** ..... 41

**September** ..... 43

**October** ..... 45

**November** ..... 48

**December** ..... 50

**Conclusion: Preparing for What Comes Next** ..... 52

**Sources Cited** ..... 53

**About LOVI** ..... 55

**About Loginsoft**..... 56

## Executive Summary: Cybersecurity Landscape in 2025

The cybersecurity landscape in 2025 was defined by faster exploitation cycles, expanding attack surfaces, and increasingly coordinated threat actor activity across enterprises, governments, and critical infrastructure. Attackers increasingly targeted software supply chains by compromising development tools, third-party components, and update mechanisms, allowing malicious code to be introduced before software reached production environments. The convergence of ransomware operations, state-aligned threat groups, and opportunistic cybercrime blurred traditional threat boundaries, making attribution and defense more complex than ever.

This report provides a comprehensive assessment of the 2025 threat environment, drawing on real-world exploitation data, malware telemetry, and vulnerability intelligence. It examines the most actively exploited CVEs, emerging malware families, and prominent threat actors observed throughout the year, highlighting how attackers chained vulnerabilities with misconfigurations, weak authentication, and insecure design to achieve persistent access.

A key focus of this report is the prioritization gap between vulnerability disclosure and active exploitation. Through detailed analysis, it demonstrates why traditional severity-based scoring alone is no longer sufficient and emphasizes the importance of threat-informed vulnerability management. Insights from Loginsoft Vulnerability Intelligence (LOVI) underpin this analysis, with continuously updated intelligence on exploited vulnerabilities, malware behavior, and threat actor profiles enabling a more proactive defense posture.

Together, these findings offer security leaders, practitioners, and decision-makers a clear, actionable understanding of 2025's cyber risk landscape, while providing strategic direction for strengthening resilience, improving detection and response, and preparing for the evolving threats of 2026.

## Ransomware Activity in 2025

Ransomware activity in 2025 reflected a clear maturation of the threat landscape, with double extortion firmly established as the default operating model. Threat actors now routinely combine data exfiltration, file encryption, and public pressure through leak sites, shifting the battle from simple recovery to regulatory, reputational, and legal risk. Despite sustained law-enforcement actions and high-profile infrastructure takedowns, Ransomware-as-a-Service (RaaS) ecosystems proved highly resilient, quickly resurfacing through rebrands, affiliate migrations, and reused tooling. These operations increasingly function like decentralized businesses, allowing campaigns to continue with minimal disruption even when individual brands collapse.

At the same time, identity-based compromise overtook vulnerability exploitation as the dominant initial access vector, fueled by credential theft, infostealer logs, and access brokers monetizing VPN, RDP, and cloud credentials. Attackers also expanded their focus beyond traditional Windows environments, with Linux and ESXi systems becoming prime targets due to their ability to cause high-impact, organization-wide disruption with relatively low effort. Looking ahead, 2025 set the stage for accelerated rebranding and ecosystem overlap in 2026, as shared codebases, affiliate reuse, and rapid mutation continue to blur the lines between ransomware “groups,” making attribution harder and defense more urgent than ever.

# New Ransomware Observed in 2025

Ransomware activity in 2025 reflected an attack ecosystem that was both expanding and rapidly evolving. The number of active ransomware groups continued to grow, while new tactics including AI-assisted extortion, file-wiping, and zero-day exploitation became increasingly prominent. At the same time, ransomware operations blurred the boundary between financially motivated crime and espionage or ideological activity, with attackers increasingly targeting critical infrastructure and cloud environments.

**Here are some of the new ransomware groups observed in 2025:**

## DOGE BIG BALLS

DOGE Big Balls is a highly distinctive ransomware variant, closely linked to the Fog ecosystem, combining technical exploitation with deliberate psychological pressure. It is uniquely delivered via phishing ZIP archives that trigger PowerShell-based payloads and stands out for abusing the ***iqvw64e.sys* vulnerable driver (CVE-2015-2291)** to achieve stealthy kernel-level privilege escalation. The ransomware performs detailed host reconnaissance, logging system intelligence to ***DbgLog.sys***, selectively encrypts user data while avoiding core Windows directories, and drops a provocative ***RANSOMNOTE.txt*** designed to amplify fear through data-leak threats. This blend of low-level exploitation, selective encryption, and intimidation-driven extortion makes DOGE Big Balls a particularly disruptive and psychologically aggressive threat.

**Vulnerabilities abused by DOGE Big Balls Ransomware:**

1. [CVE-2015-2291](#) - A Denial-of-Service vulnerability in Intel Ethernet Diagnostics Driver for Windows.
  - <https://cyble.com/blog/doge-big-balls-ransomware-edward-coristine/>

## NightSpire

NightSpire, quickly positioned itself as a high-impact ransomware actor by pairing double-extortion operations with exploitation of advanced vulnerabilities. The group maintains a dark-web leak portal with countdown-based coercion and employs stealth techniques LOLBins, MEGACmd, WinSCP to exfiltrate data while remaining undetected inside victim networks. Its campaigns span the U.S., Japan, Taiwan, Egypt, and the U.K., with a notable concentration on manufacturing, reflecting a globally distributed yet technically disciplined threat posture.

**Vulnerabilities abused by Nightspire Ransomware:**

1. [CVE-2024-55591](#) - An Authentication Bypass vulnerability in Fortinet FortiOS and FortiProxy.
  - <https://socradar.io/blog/dark-web-profile-nightspire-ransomware/>

## SuperBlack

SuperBlack is a newly emerging ransomware variant built using the leaked LockBit builder and is currently attributed to the threat actor Mora\_001, believed to be a LockBit affiliate. After gaining initial access, SuperBlack operators create persistent admin and VPN accounts, move laterally across the network, exfiltrate sensitive data, and deploy both encryption and a destructive wiper component known as WipeBlack. While confirmed victim details remain limited, the global prevalence of Fortinet appliances suggests organizations across the U.S., India, Brazil, and other regions are at elevated risk, especially in sectors heavily dependent on perimeter firewalls.

**Vulnerabilities abused by SuperBlack Ransomware:**

1. [CVE-2025-24472](#) - An Authentication Bypass vulnerability in Fortinet FortiOS and FortiProxy.

- <https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/>
2. [CVE-2024-55591](#) - An Authentication Bypass vulnerability in Fortinet FortiOS and FortiProxy.
    - <https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/>

## The Gentlemen

The Gentlemen Ransomware group has emerged as a steadily advancing threat actor known for its strategic targeting and disciplined operational methods. The group has focused heavily on organizations across 17 countries, with the Asia-Pacific region being most affected, particularly Thailand, followed by notable activity in the United States. Its campaigns have struck manufacturing the hardest, alongside construction, healthcare, insurance, and other critical service sectors, underscoring the group's willingness to disrupt essential infrastructure. To evade detection and maintain persistence, The Gentlemen relies on a blend of legitimate administrative tools, custom anti-AV utilities, and environment-tailored payloads, enabling stealthy lateral movement and long-term footholds.

### **Vulnerabilities abused by The Gentlemen Ransomware:**

1. [CVE-2025-7771](#) - A Privilege Escalation vulnerability in ThrottleStop.sys Driver.
  - [https://www.trendmicro.com/en\\_us/research/25/i/unmasking-the-gentlemen-ransomware.html](https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html)

## Warlock

Warlock Ransomware has emerged as a highly sophisticated, enterprise-focused threat actor leveraging SharePoint exploits, ToolShell attack chains, and legitimate tools like Velociraptor to maintain stealth and persistence inside victim networks. With 78 confirmed victims across the United States, Japan, and Russia, the group demonstrates a clear focus on high-value environments. Its operations span technology, infrastructure, telecommunications, finance, manufacturing, and agriculture, underscoring a broad yet strategically curated targeting profile aimed at maximizing operational and financial impact.

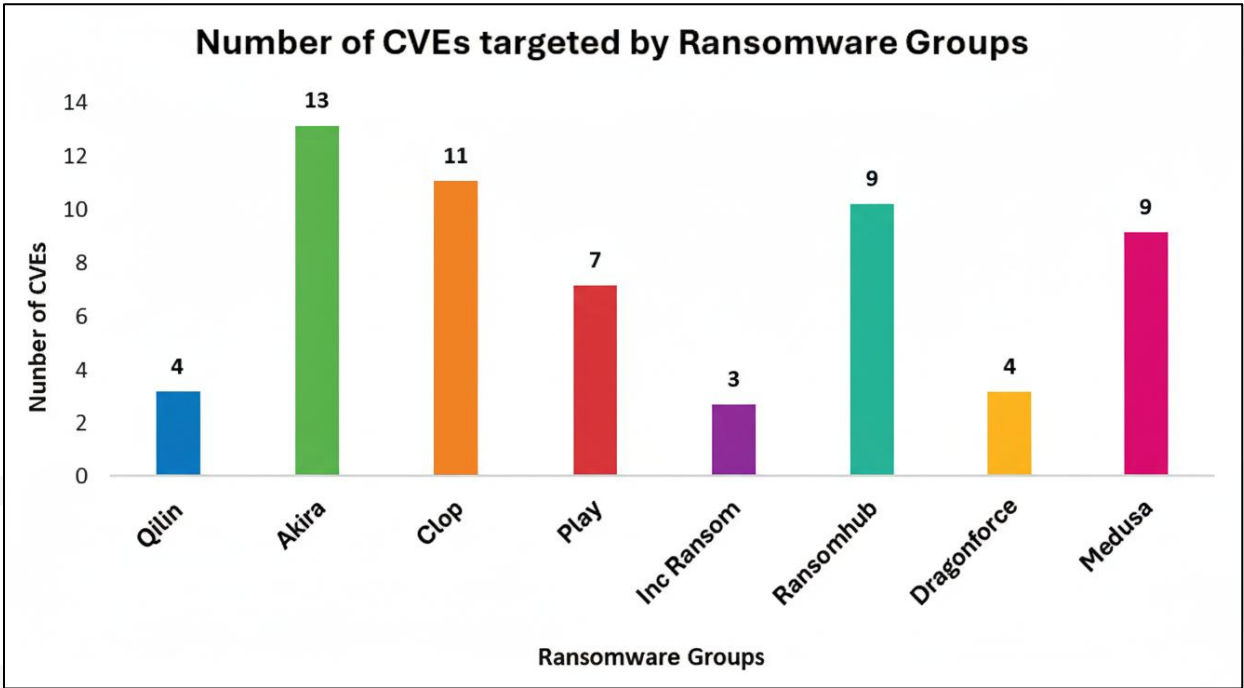
### **Vulnerabilities abused by Warlock Ransomware:**

1. [CVE-2025-49704](#) - A Code Injection vulnerability in Microsoft SharePoint Server.
  - <https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/>
2. [CVE-2025-49706](#) - An Improper Authentication vulnerability in Microsoft SharePoint Server.
  - <https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/>
3. [CVE-2025-53770](#) - A Deserialization of Untrusted Data vulnerability in Microsoft SharePoint Sever.
  - <https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/>
4. [CVE-2025-53771](#) - A Path Traversal vulnerability in Microsoft SharePoint Server.
  - <https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/>

# Ransomware Insights – 2025

In 2025, ransomware activity demonstrated unprecedented sophistication, scale, and strategic evolution. Based on proprietary research conducted by **LOGINSOFT VULNERABILITY INTELLIGENCE (LOVI)**, our telemetry reveals not only which ransomware families were most active, but also how they operated, where they struck, and which access vectors they leveraged most effectively.

By integrating LOVI’s ransomware insights into security operations, organizations can reduce attacker dwell time, strengthen proactive defenses, and build long-term resilience against an increasingly aggressive and fast-evolving ransomware landscape.



*A bar graph illustrating Number of CVEs abused by Ransomware groups - 2025*

Source: Loginsoft Vulnerability Intelligence (LOVI)

| Ransomware            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | No.of.Affected organizations<br>Jan - Dec | Top targeted Countries                                        | Targeted Industries                                                                                                                                                      | Vulnerabilities abused         |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| <a href="#">Qilin</a> | Qilin Ransomware is characterized by a highly structured and professionalized ransomware-as-a-service(RaaS) model, supported by technically mature and repeatable attack workflows. Initial access is commonly achieved through compromised credentials, exposed services, or the abuse of known weaknesses, after which a modular payload is deployed to encrypt data and disrupt business operations. The ransomware incorporates multiple evasion techniques to hinder detection and analysis, while its architecture supports flexible deployment and updates. A dedicated Tor-based portal is used for victim communication and ransom negotiation, reflecting an organized extortion framework. Multiple variants have been observed over time, indicating ongoing development and adaptation of the malware family. | 998                                       | United States<br>Canada<br>France<br>United Kingdom<br>Spain  | <ul style="list-style-type: none"> <li>• Manufacturing</li> <li>• Healthcare</li> <li>• Technology</li> <li>• Business Services</li> <li>• Financial Services</li> </ul> | <a href="#">CVE-2025-31324</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2024-21762</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2024-55591</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2023-27532</a> |
| <a href="#">Akira</a> | Akira is a ransomware-as-a-service (RaaS) operation distinguished by its early and aggressive focus on virtualized infrastructure. Beyond standard double-extortion tactics, Akira rapidly introduced a Linux encryptor specifically designed for VMware ESXi, enabling attackers to halt and encrypt large numbers of virtual machines from a single hypervisor using VM-aware options like vmonly and stopvm. Post-compromise activity prioritizes identity systems, backup platforms, and hypervisors, allowing fast, high-impact disruption of entire environments. This hypervisor-centric design, combined with data exfiltration via tools like rclone and SCP, makes Akira particularly effective against modern, virtualization-heavy networks.                                                                   | 732                                       | United States<br>Canada<br>Germany<br>Italy<br>United Kingdom | <ul style="list-style-type: none"> <li>• Manufacturing</li> <li>• Business Services</li> <li>• Technology</li> <li>• Construction</li> <li>• Agriculture</li> </ul>      | <a href="#">CVE-2024-37085</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2024-40711</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2024-40766</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2023-20269</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2023-20363</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2023-27532</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2023-28252</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2023-48788</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2022-40684</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2021-21972</a> |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2020-3259</a>  |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2020-3580</a>  |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                           |                                                               |                                                                                                                                                                          | <a href="#">CVE-2019-6693</a>  |

| Ransomware           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | No.of.Affected organizations<br>Jan - Dec | Top targeted Countries                                            | Targeted Industries                                                                                                                                          | Vulnerabilities abused         |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| <a href="#">ClOp</a> | <p>ClOp Ransomware originated as an evolution of the CryptoMix malware family and first emerged in early 2019, quickly establishing itself as a sophisticated and financially motivated threat. Commonly associated with the TA505/FIN11 ecosystem and tracked clusters such as UNCA2546 and UNCA2582, ClOp operates under a ransomware-as-a-service (RaaS) model and has been used in high-impact attacks against large enterprises. Technically, ClOp stands out for its use of digitally signed Win32 PE executables to appear legitimate and evade security controls, combined with strong encryption using RC4 for file data and RSA-1024 for key protection. Beyond encryption, ClOp relies heavily on double-extortion tactics, threatening public data leaks if ransom demands typically paid in cryptocurrency are not met, making it both disruptive and coercive.</p>              | 518                                       | United States<br>Canada<br>Germany<br>United Kingdom<br>Australia | <ul style="list-style-type: none"> <li>Technology</li> <li>Logistics</li> <li>Manufacturing</li> <li>Consumer Services</li> <li>Business Services</li> </ul> | <a href="#">CVE-2023-0669</a>  |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2023-34362</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2023-27350</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2023-27351</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2023-35036</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2023-47246</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2021-27101</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2021-27102</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2021-27103</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2021-27104</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2021-35211</a> |
| <a href="#">Play</a> | <p>Play Ransomware (aka Playcrypt), first observed in mid-2022, is a highly disruptive ransomware family known for its multi-extortion strategy, combining data encryption with threats of public data leaks on TOR-based sites. The group primarily gains initial access through vulnerability exploitation and exposed or rented RDP servers, with a notable focus on Fortinet FortiOS flaws and ProxyNotShell exploits. Once inside, Play emphasizes stealth and evasion, heavily leveraging LOLBins, COTS tools, intermittent encryption, and Active Directory abuse via GPOs to spread laterally. Its use of specialized tools like Grixba and AlphaVSS, along with commodity frameworks such as Cobalt Strike and Mimikatz, highlights a mature, operationally disciplined ransomware operation capable of targeting governments, enterprises, and critical institutions worldwide.</p> | 374                                       | United States<br>Canada<br>United Kingdom<br>Germany<br>Sweden    | <ul style="list-style-type: none"> <li>Manufacturing</li> <li>Business Services</li> <li>Technology</li> <li>Construction</li> <li>Logistics</li> </ul>      | <a href="#">CVE-2024-57727</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2022-41040</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2022-41080</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2022-41082</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2021-34523</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2020-12812</a> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                           |                                                                   |                                                                                                                                                              | <a href="#">CVE-2018-13379</a> |

| Ransomware                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | No.of.Affected organizations<br>Jan - Dec | Top targeted Countries                                            | Targeted Industries                                                                                                                                             | Vulnerabilities abused                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <a href="#">SafePay</a>    | SafePay Ransomware is an emerging and previously undocumented threat, first observed in October 2024, that relies heavily on valid credentials likely sourced from dark web marketplaces and VPN access to infiltrate target environments. The group employs a multi-stage intrusion chain, commonly initiating attacks via Remote Desktop Protocol (RDP) and exploiting known VPN vulnerabilities while disabling defenses such as Windows Defender using LOLbins. SafePay features a modular and sophisticated design, enabling privilege escalation, UAC bypass, and network propagation, demonstrating a high degree of operational maturity. The ransomware encrypts files with a .safepay extension and drops a readme_safepay.txt ransom note, signaling the rise of a globally active ransomware operation targeting diverse industries across multiple countries. | 365                                       | United States<br>Germany<br>United Kingdom<br>Canada<br>Australia | <ul style="list-style-type: none"> <li>• Manufacturing</li> <li>• Technology</li> <li>• Education</li> <li>• Healthcare</li> <li>• Business Services</li> </ul> | Unknown                                                                                          |
| <a href="#">Inc Ransom</a> | INC is a ransomware-as-a-service (RaaS) operation that emerged in mid-to-late 2023, operating through an affiliate-driven model in which core operators supply the malware and infrastructure while affiliates conduct intrusions and share profits. The group relies on a double-extortion strategy, coercing victims by threatening data leaks under the pretext of “protecting their reputation.” INC maintains two dedicated leak sites a private, credential-protected portal used for victim communication and negotiation, and a public site used to release stolen data. First detected in July 2023 and tracked by Trend Micro as Water Anito, the ransomware encrypts files using AES algorithm, reinforcing its position as a structured and professionally run extortion operation.                                                                            | 364                                       | United States<br>Canada<br>Germany<br>United Kingdom<br>Australia | <ul style="list-style-type: none"> <li>• Healthcare</li> <li>• Technology</li> <li>• Business Services</li> <li>• Manufacturing</li> <li>• Education</li> </ul> | <a href="#">CVE-2023-3519</a><br><a href="#">CVE-2023-4966</a><br><a href="#">CVE-2023-48788</a> |
| <a href="#">Lynx</a>       | Lynx is a ransomware group that surfaced in mid-2024 and is widely assessed to be a rebrand of the INC ransomware operation,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 242                                       | United States<br>United Kingdom<br>Canada<br>Germany              | <ul style="list-style-type: none"> <li>• Manufacturing</li> <li>• Business Services</li> <li>• Technology</li> </ul>                                            | Unknown                                                                                          |

| Ransomware                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | No.of.Affected organizations<br>Jan - Dec | Top targeted Countries                                           | Targeted Industries                                                                                                                                      | Vulnerabilities abused         |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
|                             | based on strong code-level overlaps between the two strains. Operating under a Ransomware-as-a-Service (RaaS) model, Lynx equips affiliates with encryption tooling, leak-site infrastructure, and operational support, allowing campaigns to scale rapidly. Rather than relying on a single intrusion vector, affiliates commonly gain access through stolen credentials often sourced from dark-web markets or infostealer logs and phishing attacks, enabling direct entry into RDP, VPN, and email environments. This combination of inherited code, flexible access methods, and an affiliate-driven ecosystem positions Lynx as a fast-moving and adaptable ransomware threat.                                                                                                                                                                                      |                                           | Australia                                                        | <ul style="list-style-type: none"> <li>Logistics</li> <li>Agriculture</li> </ul>                                                                         |                                |
| <a href="#">RansomHub</a>   | RansomHub is a modern ransomware-as-a-service (RaaS) operation that emerged in early 2024, quickly gaining prominence by positioning itself as a successor to disrupted groups like ALPHV/BlackCat. Operating through an affiliate-based model, RansomHub emphasizes high operational security, enforcing strict rules on affiliates such as bans on targeting certain regions to reduce law-enforcement pressure. A defining feature of RansomHub is its focus on data exfiltration and double extortion, often prioritizing data theft over encryption speed, alongside the use of custom-built encryption tooling rather than widely reused ransomware builders. Its rapid growth, disciplined affiliate management, and aggressive leak-site operations have made RansomHub one of the most active and disruptive ransomware players in the current threat landscape. | 222                                       | United States<br>Brazil<br>Canada<br>United Kingdom<br>Italy     | <ul style="list-style-type: none"> <li>Business Services</li> <li>Technology</li> <li>Manufacturing</li> <li>Healthcare</li> <li>Government</li> </ul>   | <a href="#">CVE-2023-3519</a>  |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                           |                                                                  |                                                                                                                                                          | <a href="#">CVE-2023-22515</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                           |                                                                  |                                                                                                                                                          | <a href="#">CVE-2023-27997</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                           |                                                                  |                                                                                                                                                          | <a href="#">CVE-2023-46604</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                           |                                                                  |                                                                                                                                                          | <a href="#">CVE-2023-46747</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                           |                                                                  |                                                                                                                                                          | <a href="#">CVE-2023-48788</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                           |                                                                  |                                                                                                                                                          | <a href="#">CVE-2020-0787</a>  |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                           |                                                                  |                                                                                                                                                          | <a href="#">CVE-2020-1472</a>  |
| <a href="#">DragonForce</a> | DragonForce is a ransomware group originating from Malaysia. Initially, known as a hacktivist group, DragonForce has transitioned into a ransomware operation, threatening victims with data encryption and                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 221                                       | United States<br>United Kingdom<br>Germany<br>Australia<br>Italy | <ul style="list-style-type: none"> <li>Manufacturing</li> <li>Business Services</li> <li>Technology</li> <li>Healthcare</li> <li>Construction</li> </ul> | <a href="#">CVE-2024-57726</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                           |                                                                  |                                                                                                                                                          | <a href="#">CVE-2024-57727</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                           |                                                                  |                                                                                                                                                          | <a href="#">CVE-2024-57728</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                           |                                                                  |                                                                                                                                                          | <a href="#">CVE-2022-26134</a> |

| Ransomware             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | No.of.Affected organizations<br>Jan - Dec | Top targeted Countries                                     | Targeted Industries                                                                                                                                                | Vulnerabilities abused |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|                        | extortion demands. They have targeted various industries and organizations globally, including government entities, businesses, and critical infrastructure sectors. The group gained attention for their attacks on American companies, with details about data compromise and motives undisclosed. DragonForce has also threatened to release stolen information on dark web leak sites to pressure victims into paying ransoms.                                                                                                                                                                                                                                                                        |                                           |                                                            |                                                                                                                                                                    |                        |
| <a href="#">Sinobi</a> | Sinobi ransomware is a sophisticated threat, suspected to be a rebrand of the Lynx ransomware group, employing double-extortion tactics that exfiltrate sensitive data before encrypting systems using Curve-25519 and AES-128-CTR algorithms. It has targeted a wide range of industries, including healthcare, manufacturing, legal services, education, and construction/engineering, highlighting its broad attack strategy. To mitigate risk, organizations are advised to implement multi-factor authentication, secure VPN access, keep systems updated with patches, train employees on phishing and safe practices, maintain offline backups, and monitor network activity for unusual behavior. | 187                                       | United States<br>United Kingdom<br>India<br>Italy<br>Spain | <ul style="list-style-type: none"> <li>• Healthcare</li> <li>• Manufacturing</li> <li>• Construction</li> <li>• Technology</li> <li>• Business Services</li> </ul> | Unknown                |
| <a href="#">DevMan</a> | DevMan Ransomware is characterized by its opportunistic yet technically efficient attack model, often targeting exposed services and misconfigured systems for rapid intrusion. The malware emphasizes fast execution, combining credential harvesting and lightweight lateral movement before deploying its encryption payload. DevMan typically incorporates data exfiltration to support double-extortion tactics, increasing pressure during ransom negotiations. Its tooling is streamlined to reduce operational noise while maintaining persistence and                                                                                                                                            | 155                                       | United States<br>France<br>Taiwan<br>Thailand<br>China     | <ul style="list-style-type: none"> <li>• Technology</li> <li>• Healthcare</li> <li>• Public Sector</li> <li>• Construction</li> <li>• Agriculture</li> </ul>       | Unknown                |

| Ransomware                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | No.of.Affected organizations<br>Jan - Dec | Top targeted Countries                                          | Targeted Industries                                                                                                                                               | Vulnerabilities abused         |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
|                             | control over compromised environments.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                           |                                                                 |                                                                                                                                                                   |                                |
| <a href="#">Medusa</a>      | Medusa is a distinct ransomware operation known for appending the <b>.medusa</b> file extension to encrypted data and dropping a customized ransom note directing victims to its Tor-based negotiation portal. Unlike many groups, Medusa is notable for its public leak site countdown timers, which visibly pressure victims by displaying deadlines before stolen data is released. The group places heavy emphasis on data exfiltration-first attacks, often stealing large volumes of sensitive information before encryption begins. Medusa has also gained attention for pairing extortion with public shaming tactics and threats of secondary consequences, making its campaigns psychologically aggressive as well as technically disruptive. | 152                                       | United States<br>Canada<br>United Kingdom<br>Australia<br>Italy | <ul style="list-style-type: none"> <li>• Business Services</li> <li>• Healthcare</li> <li>• Manufacturing</li> <li>• Technology</li> <li>• Government</li> </ul>  | <a href="#">CVE-2024-1709</a>  |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                           |                                                                 |                                                                                                                                                                   | <a href="#">CVE-2024-37085</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                           |                                                                 |                                                                                                                                                                   | <a href="#">CVE-2022-2294</a>  |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                           |                                                                 |                                                                                                                                                                   | <a href="#">CVE-2022-2295</a>  |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                           |                                                                 |                                                                                                                                                                   | <a href="#">CVE-2023-4966</a>  |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                           |                                                                 |                                                                                                                                                                   | <a href="#">CVE-2023-48788</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                           |                                                                 |                                                                                                                                                                   | <a href="#">CVE-2022-21999</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                           |                                                                 |                                                                                                                                                                   | <a href="#">CVE-2021-34473</a> |
|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                           |                                                                 |                                                                                                                                                                   | <a href="#">CVE-2018-13379</a> |
| <a href="#">KillSec</a>     | KillSec is a hacktivist-aligned ransomware operation that blends data destruction, extortion, and ideological messaging, setting it apart from purely profit-driven groups. The ransomware is known to append the <b>.killsec</b> file extension to encrypted files and deploy stark ransom notes that often include political or retaliatory rhetoric alongside payment demands. KillSec places strong emphasis on public data leaks and reputational damage, frequently publishing stolen information even when ransom negotiations stall. This fusion of ransomware tactics with hacktivist objectives makes KillSec particularly unpredictable and disruptive compared to traditional RaaS operations.                                              | 126                                       | United States<br>India<br>United Kingdom<br>Brazil<br>Belgium   | <ul style="list-style-type: none"> <li>• Healthcare</li> <li>• Technology</li> <li>• Business Services</li> <li>• Financial Services</li> </ul>                   | Unknown                        |
| <a href="#">World Leaks</a> | World Leaks is a data-leak-centric extortion operation that differentiates itself by prioritizing theft and public disclosure over large-scale file encryption. Rather than relying solely on classic ransomware deployment, WorldLeaks is known for                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 112                                       | United States<br>Canada<br>United Kingdom<br>Brazil<br>Germany  | <ul style="list-style-type: none"> <li>• Healthcare</li> <li>• Manufacturing</li> <li>• Technology</li> <li>• Consumer Services</li> <li>• Hospitality</li> </ul> | Unknown                        |

| Ransomware | Description                                                                                                                                                                                                                                                                                                                                                                                                                         | No.of.Affected organizations<br>Jan - Dec | Top targeted Countries | Targeted Industries | Vulnerabilities abused |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|------------------------|---------------------|------------------------|
|            | aggressively publishing stolen data on its leak platform to maximize reputational and regulatory pressure on victims. The group often skips full encryption altogether or uses selective encryption, signaling a strategic shift toward “leakware”-style extortion. This approach allows WorldLeaks to move faster, reduce operational noise, and still achieve high-impact coercion through exposure rather than disruption alone. |                                           |                        |                     |                        |

## What can we expect from Ransomware in 2026?

As ransomware operations continue to mature, 2026 is poised to be defined by speed, access, and adaptability rather than novelty. Ransomware groups are increasingly behaving like brands rather than fixed organizations, rapidly rebranding when faced with law-enforcement pressure, internal leaks, or reputational damage. This normalization of rebranding will accelerate mutation cycles, affiliate reuse, and infrastructure overlap, making attribution harder and disruption less effective. At the same time, double extortion is evolving into full-scale, multi-stage extortion, where encryption and data theft are merely the baseline. Threat actors are expected to layer on DDoS threats, executive harassment, partner and vendor pressure, regulatory exposure threats, and insider-style coercion, significantly intensifying negotiation pressure on victims.

From an access perspective, identity will remain on the primary attack surface. Compromised VPNs, RDP, cloud identities, and stolen credentials already dominate initial access, and credential access brokers are expected to expand further in 2026, feeding ransomware affiliates at scale. Technically, attackers will increasingly favor Linux and hypervisor environments, particularly ESXi, due to their ability to cause immediate, organization-wide disruption with a single intrusion. Rather than a few dominant mega-groups, the ecosystem will likely shift toward smaller, agile crews that reuse tooling, scale via affiliates, strike quickly, and disappear resulting in many smaller but highly damaging incidents instead of a single dominant threat actor.

## How organizations can prepare and how LOVI helps

In this environment, success in 2026 will depend less on tracking ransomware names and more on understanding attacker behavior, access paths, and lateral movement. This is where **Loginsoft Vulnerability Intelligence (LOVI)** becomes critical. LOVI provides early visibility into exploited vulnerabilities, identity-based exposure, ransomware trends, and ecosystem overlaps, enabling organizations to move from reactive defense to proactive risk reduction. By correlating ransomware activity with real-world exploitation patterns, access techniques, and victim trends, LOVI helps security teams prioritize credential hygiene, exposure management, patch discipline, behavioral detection, and proactive leak-site monitoring. As ransomware evolves into a repeatable business process, LOVI equips organizations with the intelligence needed to break attacker playbooks early before access turns into impact.

# Most Observed Vulnerabilities from our Sensors

Intel collected through our LOVI platform powered by honeypot sensors distributed across diverse geographic regions has revealed critical insights into emerging threat activity. These sensors have captured extensive exploitation attempts tied to multiple CVEs, offering a clear view of how attackers operate in real-world environments. This distributed monitoring approach not only uncovered regional differences in attack behavior but also reinforces the value of wide-scale sensor networks for early detection and effective risk mitigation.

| CVE-ID                         | Vendor                     | Product                                         | Severity | Description                                                                                                                                                                                                                                    |
|--------------------------------|----------------------------|-------------------------------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">CVE-2025-7417</a>  | Tenda                      | O3V2 router                                     | High     | A Stack-Based Buffer Overflow vulnerability in the Tenda O3V2 1.0.0.12(3880)                                                                                                                                                                   |
| <a href="#">CVE-2025-7414</a>  | Tenda                      | O3V2 router                                     | High     | An OS Command Injection vulnerability in the Tenda O3V2 1.0.0.12(3880)                                                                                                                                                                         |
| <a href="#">CVE-2025-61882</a> | Oracle                     | E-Business Suite                                | Critical | An Improper Authentication vulnerability in the Oracle E-Business Suite allows unauthenticated attacker with network access via HTTP to compromise Oracle Concurrent Processing.                                                               |
| <a href="#">CVE-2025-5777</a>  | Citrix                     | NetScaler ADC and Gateway                       | Critical | An Out-of-Bounds Read vulnerability in Citrix NetScaler ADC and Gateway that arises due to insufficient input validation.                                                                                                                      |
| <a href="#">CVE-2025-3248</a>  | Langflow                   | Langflow                                        | Critical | A Missing Authentication vulnerability in the Langflow in the /api/v1/validate/code endpoint that allows a remote, unauthenticated attacker to execute arbitrary code via crafted HTTP requests.                                               |
| <a href="#">CVE-2025-32432</a> | Craft CMS                  | Craft CMS                                       | Critical | A Remote Code Execution vulnerability in the Craft CMS enables attackers to send specially crafted requests.                                                                                                                                   |
| <a href="#">CVE-2025-31324</a> | SAP                        | NetWeaver                                       | Critical | An Unrestricted File Upload vulnerability in the SAP NetWeaver Visual Composer Metadata Uploader that allows an unauthenticated agent to upload potentially malicious executable binaries.                                                     |
| <a href="#">CVE-2025-27636</a> | Apache Software Foundation | Camel                                           | Medium   | An Improper Handling of Case Sensitivity vulnerability in the Apache Camel components under particular conditions.                                                                                                                             |
| <a href="#">CVE-2025-26399</a> | SolarWinds                 | Web Help Desk                                   | Critical | Deserialization of Untrusted Data vulnerability in SolarWinds Web Help Desk that, if exploited, would allow an attacker to run commands on the host machine.                                                                                   |
| <a href="#">CVE-2025-25257</a> | Fortinet                   | FortiWeb                                        | Critical | A SQL Injection vulnerability in the Fortinet FortiWeb that may allow an unauthenticated attacker to execute unauthorized SQL code or commands via crafted HTTP or HTTPs requests.                                                             |
| <a href="#">CVE-2025-22457</a> | Ivanti                     | Connect Secure, Policy Secure, and ZTA Gateways | Critical | A Stack-Based Buffer Overflow vulnerability in the Ivanti Connect Secure, Policy Secure, and ZTA Gateways contains a stack-based buffer overflow vulnerability that allows a remote unauthenticated attacker to achieve remote code execution. |
| <a href="#">CVE-2024-8503</a>  | VICIdial Group             | VICIdial                                        | Critical | An SQL Injection vulnerability in the VICIdial 2.14-917a leads to sensitive information disclosure                                                                                                                                             |
| <a href="#">CVE-2024-6782</a>  | Calibre                    | Calibre                                         | Critical | An Improper Access Control vulnerability in the Calibre that allows unauthenticated attackers to achieve remote code execution through the content server feature.                                                                             |
| <a href="#">CVE-2024-47176</a> | CUPS                       | CUPS                                            | Medium   | Binding to an Unrestricted IP Address vulnerability in the CUPS that allows an attacker to execute arbitrary commands remotely on the target machine without authentication when a malicious printer is printed to.                            |
| <a href="#">CVE-2024-4577</a>  | PHP Group                  | PHP                                             | Critical | An OS Command Injection vulnerability in PHP, specifically Windows-based PHP used in CGI mode, that allows for arbitrary code execution.                                                                                                       |

# Opensource Software Vulnerabilities abused by Threat Actors

OSS Intelligence involves gathering and analyzing information about vulnerabilities across all available opensource packages. The LOVI platform plays a key role in this process by utilizing its extensive OSS databases, which offer comprehensive coverage of all CVEs. To ensure that high-risk vulnerabilities are prioritized, LOVI further segments and categorizes the CVEs, focusing on the most critical and trending issues. The platform supports various open-source ecosystems, including Maven, Alpine, Debian, Android, RubyGems, NuGet, Linux, GSD, and Packagist, among others, enabling thorough tracking and management of vulnerabilities across multiple environments.

| CVE-ID                         | Vendor             | Product      | Severity | Description                                                          | Abused by Malware                |
|--------------------------------|--------------------|--------------|----------|----------------------------------------------------------------------|----------------------------------|
| <a href="#">CVE-2025-3248</a>  | Langflow           | Langflow     | Critical | A Missing Authentication vulnerability in Langflow                   | <a href="#">Flodrix Botnet</a>   |
| <a href="#">CVE-2025-24016</a> | Wazuh              | Wazuh Server | Critical | A Deserialization of Untrusted Data vulnerability in Wazuh Server    | <a href="#">Mirai</a>            |
| <a href="#">CVE-2025-32432</a> | Craft              | CMS          | Critical | A Code Injection vulnerability in the Craft CMS                      | <a href="#">Mimo Loader</a>      |
| <a href="#">CVE-2024-3400</a>  | Palo Alto Networks | PAN-OS       | Critical | A Command Injection vulnerability in the Palo Alto Networks PAN-OS   | <a href="#">XMRig Miner</a>      |
|                                |                    |              |          |                                                                      | <a href="#">Silk Typhoon</a>     |
|                                |                    |              |          |                                                                      | <a href="#">Black Basta</a>      |
|                                |                    |              |          |                                                                      | <a href="#">Fox Kitten</a>       |
|                                |                    |              |          |                                                                      | <a href="#">RedTail</a>          |
|                                |                    |              |          |                                                                      | <a href="#">UTA0218</a>          |
|                                |                    |              |          |                                                                      | <a href="#">UPSTYLE</a>          |
|                                |                    |              |          |                                                                      | <a href="#">Earth Estries</a>    |
| <a href="#">CVE-2024-38475</a> | Apache             | HTTP server  | Critical | An Improper Escaping of Output vulnerability in Apache HTTP server   | <a href="#">OVERSTEP</a>         |
| <a href="#">CVE-2024-42009</a> | RoundCube          | Webmail      | Critical | A Cross-Site Scripting vulnerability in RoundCube Webmail            | <a href="#">UNC6148</a>          |
| <a href="#">CVE-2024-50302</a> | Linux              | Kernel       | Medium   | A Use of Uninitialized Resource vulnerability in Linux Kernel        | <a href="#">UNC1151</a>          |
| <a href="#">CVE-2024-53104</a> | Linux              | Kernel       | High     | An Out-of-Bounds Write vulnerability in Linux Kernel                 | <a href="#">NoviSpy</a>          |
| <a href="#">CVE-2023-46604</a> | Apache             | ActiveMQ     | Critical | A Deserialization of Untrusted Data vulnerability in Apache ActiveMQ | <a href="#">Mauri Ransomware</a> |
|                                |                    |              |          |                                                                      | <a href="#">RansomHub</a>        |
|                                |                    |              |          |                                                                      | <a href="#">KrustyLoader</a>     |
|                                |                    |              |          |                                                                      | <a href="#">Mimo CoinMiner</a>   |

# CISA Industrial Control Systems (ICS) General CVE's abused by Malware

CISA ICS refers to CISA’s specialized mission area focused on helping critical infrastructure operators manage and reduce cyber risks in Industrial Control Systems. It serves as the U.S. government’s lead civilian authority for ICS security guidance, threat intelligence, and incident response. Through advisories, assessments, and best-practice frameworks, CISA ICS supports sectors like energy, water, manufacturing, and transportation in strengthening OT resilience against cyber threats.

| CVE-ID                         | Vendor             | Product                       | Severity | Description                                                                                                                                                                                                                                   | Malware Abused                                                                                                                                                                                           |
|--------------------------------|--------------------|-------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">CVE-2025-0411</a>  | 7-Zip              | 7-Zip                         | High     | A Mark of the Web Bypass vulnerability in the 7-Zip allows remote attackers to execute arbitrary code with the privileges of the current user.                                                                                                | <a href="#">SmokeLoader</a>                                                                                                                                                                              |
| <a href="#">CVE-2025-0994</a>  | Trimble            | Cityworks                     | High     | A Deserialization vulnerability in Trimble Cityworks that enables an authenticated user to perform remote code execution.                                                                                                                     | <a href="#">UAT-6382</a><br><a href="#">China Chopper</a><br><a href="#">VSHell</a>                                                                                                                      |
| <a href="#">CVE-2025-1316</a>  | Edimax             | IC-7100 IP Camera             | Critical | An OS Command Injection vulnerability in the Edimax IC-7100 IP Camera due to improper input sanitization that allows an attacker to achieve remote code execution via specially crafted requests.                                             | <a href="#">Mirai</a>                                                                                                                                                                                    |
| <a href="#">CVE-2025-6554</a>  | Google             | Chrome                        | High     | Type Confusion vulnerability in Google Chrome                                                                                                                                                                                                 | <a href="#">Predator</a>                                                                                                                                                                                 |
| <a href="#">CVE-2025-20352</a> | Cisco              | IOS and IOS XE Software       | High     | An SNMP Denial of Service and Remote Code Execution vulnerability in the Cisco IOS and IOS XE Software that could allow a high-privileged attacker to execute arbitrary code as the root user and obtain full control of the affected system. | <a href="#">Operation Zero Disco</a>                                                                                                                                                                     |
| <a href="#">CVE-2025-22224</a> | VMware             | ESXi Workstation              | Critical | A Race Condition vulnerability in VMware ESXi and Workstation leads to out of bounds write                                                                                                                                                    | <a href="#">APT28</a><br><a href="#">APT29</a><br><a href="#">APT41</a>                                                                                                                                  |
| <a href="#">CVE-2025-22225</a> | VMware             | ESXi                          | High     | Arbitrary Write vulnerability in VMware ESX                                                                                                                                                                                                   | <a href="#">APT28</a><br><a href="#">APT29</a><br><a href="#">APT41</a>                                                                                                                                  |
| <a href="#">CVE-2025-22226</a> | VMware             | ESXi, Workstation, and Fusion | High     | An Information Disclosure vulnerability in the VMware ESXi, Workstation, and Fusion allows an attacker with administrative privileges to a virtual machine to leak memory from the vmx process.                                               | <a href="#">APT28</a><br><a href="#">APT29</a><br><a href="#">APT41</a>                                                                                                                                  |
| <a href="#">CVE-2025-59287</a> | Microsoft          | Windows                       | Critical | Deserialization of Untrusted Data vulnerability in the Microsoft Windows Server Update Service (WSUS)                                                                                                                                         | <a href="#">ShadowPad</a>                                                                                                                                                                                |
| <a href="#">CVE-2024-0012</a>  | Palo Alto Networks | PAN-OS                        | Critical | An Authentication Bypass vulnerability in the Palo Alto Networks PAN-OS Management Interface                                                                                                                                                  | <a href="#">DEV-0401</a><br><a href="#">Mustang Panda</a><br><a href="#">MgBot</a><br><a href="#">PlugX</a><br><a href="#">RA Group</a><br><a href="#">XMRig</a><br><a href="#">OPERATION LUNAR PEEK</a> |

| CVE-ID                         | Vendor                      | Product               | Severity | Description                                                                                                                                                                                                                                                    | Malware Abused               |
|--------------------------------|-----------------------------|-----------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <a href="#">CVE-2024-1086</a>  | Linux                       | Kernel                | High     | A Use-After-Free vulnerability in Linux Kernel                                                                                                                                                                                                                 | <a href="#">Black Basta</a>  |
| <a href="#">CVE-2024-2961</a>  | GNU C Library               | GNU C Library         | High     | An Out-of-bounds Write vulnerability in <b>iconv() function</b> in the GNU C Library leads to remote code execution, buffer overflow                                                                                                                           | <a href="#">MageCart</a>     |
| <a href="#">CVE-2024-3400</a>  | Palo Alto Networks          | PAN-OS                | Critical | A Command Injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS                                                                                                                                                                    | <a href="#">Fox Kitten</a>   |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">HAFNIUM</a>      |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">UTA0218</a>      |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">Black Basta</a>  |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">RedTail</a>      |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">UPSTYLE</a>      |
| <a href="#">CVE-2024-7029</a>  | AVTECH SECURITY Corporation | IP Camera             | Critical | A Command Injection vulnerability in the AVTECH IP Camera                                                                                                                                                                                                      | <a href="#">Murdoc</a>       |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">Mirai</a>        |
| <a href="#">CVE-2024-8956</a>  | PTZOptics                   | PT30X-SDI/NDI Cameras | Critical | An Authentication Bypass vulnerability in the PTZOptics PT30X-SDI/NDI Cameras that allows a remote, attacker to bypass authentication for the <b>/cgi-bin/param.cgi</b> CGI script.                                                                            | <a href="#">Gayfemboy</a>    |
| <a href="#">CVE-2024-8957</a>  | PTZOptics                   | PT30X-SDI/NDI Cameras | High     | An OS Command Injection vulnerability in the PTZOptics PT30X-SDI/NDI Cameras that allows a remote, authenticated attacker to escalate privileges to root via a crafted payload with the <b>ntp_addr</b> parameter of the <b>/cgi-bin/param.cgi</b> CGI script. | <a href="#">Gayfemboy</a>    |
| <a href="#">CVE-2024-21762</a> | Fortinet                    | FortiOS               | Critical | An Out-of-Bounds Write vulnerability in the Fortinet FortiOS allows a remote unauthenticated attacker to execute code or commands via specially crafted HTTP requests.                                                                                         | <a href="#">Qilin</a>        |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">Black Basta</a>  |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">Mirai</a>        |
| <a href="#">CVE-2024-50302</a> | Linux                       | Kernel                | Medium   | A Use of Uninitialized Resource vulnerability in the Linux Kernel that allows an attacker to leak kernel memory via a specially crafted HID report.                                                                                                            | <a href="#">NoviSpy</a>      |
| <a href="#">CVE-2024-53104</a> | Linux                       | Kernel                | High     | An Out-of-Bounds Write vulnerability in the Linux Kernel that allows for physical escalation of privilege.                                                                                                                                                     | <a href="#">NoviSpy</a>      |
| <a href="#">CVE-2024-53197</a> | Linux                       | Kernel                | High     | An Out-of-Bounds Access vulnerability in the Linux Kernel that allows an attacker with physical access to the system to use a malicious USB device to potentially manipulate system memory, escalate privileges, or execute arbitrary code.                    | <a href="#">NoviSpy</a>      |
| <a href="#">CVE-2023-4911</a>  | GNU                         | GNU C Library         | High     | Buffer overflow vulnerability in GNU C Library's dynamic loader                                                                                                                                                                                                | <a href="#">Kinsing</a>      |
| <a href="#">CVE-2023-46604</a> | Apache                      | ActiveMQ              | Critical | Deserialization of untrusted data vulnerability in Apache ActiveMQ                                                                                                                                                                                             | <a href="#">Mauri</a>        |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">RansomHub</a>    |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">KrustyLoader</a> |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">Kinsing</a>      |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">Mimo</a>         |
|                                |                             |                       |          |                                                                                                                                                                                                                                                                | <a href="#">Mimus</a>        |

# Threat Activity Landscape in 2025

The threat landscape in 2025 continued to evolve at a rapid pace, driven by increasingly agile threat actors and the accelerated exploitation of newly disclosed vulnerabilities. Throughout the year, more than 40 new malware families and variants were identified, actively exploiting vulnerabilities across a wide range of products and technologies. These campaigns targeted enterprise networks, cloud workloads, and edge-facing applications, with attackers frequently weaponizing freshly published CVEs within days of disclosure. Observed malware spanned multiple categories including botnets, spyware, and remote access trojans (RATs) with notable examples such as Gayfemboy botnet, Airashi botnet, StormKitty, Rustobot, Landfall, PurpleHaze, Storm-2603, the Xe group, and several others. Zero-day exploitation, abuse of perimeter devices, and chaining of low-complexity flaws into high-impact intrusion paths emerged as defining characteristics of modern campaigns. In many cases, malware operators demonstrated a deep understanding of victim environments, leveraging misconfigurations, identity weaknesses, and unpatched software to achieve persistence and lateral movement.

To keep pace with this shifting threat landscape, **LOGINSOFT VULNERABILITY INTELLIGENCE** (LOVI) played a critical role in tracking emerging malware activity and the vulnerabilities most frequently abused in real-world attacks. LOVI researchers continuously monitor malware campaigns, exploit trends, and CVE weaponization patterns, ensuring that intelligence is updated as new threats surface. By correlating malware behaviour with exploited CVEs and attack chains, LOVI enables security teams to move beyond reactive patching and adopt a proactive, intelligence-driven defense strategy prioritizing vulnerabilities that matter most in 2025's active threat environment.

## Active Malware and Threat Actors in 2025

The following section presents some of the newly observed malware families and prominent threat actors active in 2025, along with the critical vulnerabilities (CVEs) they exploited in real-world attack campaigns. By correlating malware behavior, attacker tradecraft, and vulnerability weaponization, this analysis provides deeper insight into evolving exploitation techniques.

Each malware family and threat actor is supported by a dedicated, continuously updated threat profile within LOVI, offering actionable intelligence on exploitation patterns, tooling, and attribution.

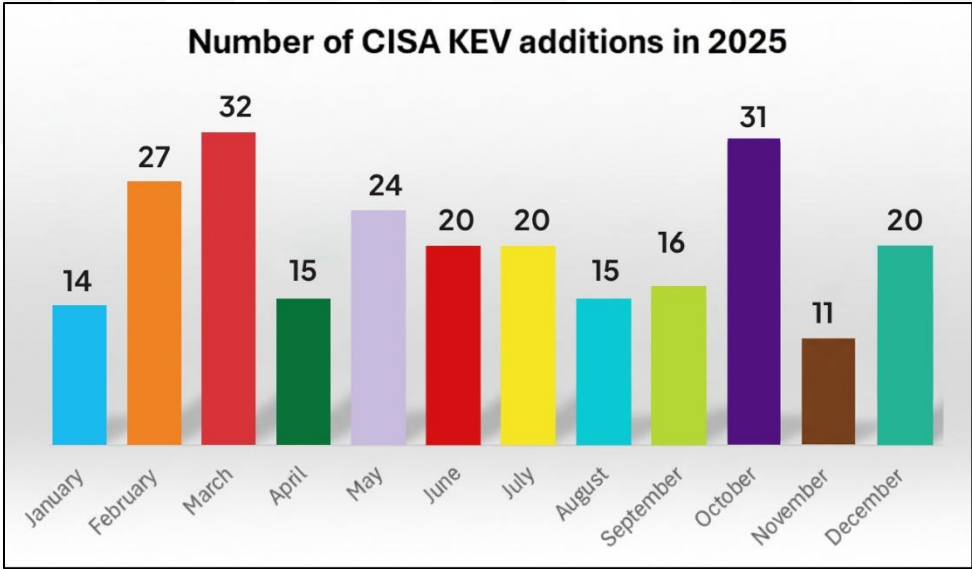
| Name                         | Description                                                                                                                                                                                                                                                                                                                                                                                     | Vulnerabilities Abused         |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| <a href="#">Ballista</a>     | The Ballista botnet leverages a command injection flaw in TP-Link Archer routers' web interface, enabling unauthenticated root-level code execution. It exploits unsanitized input in the <code>/cgi-bin/luci;stok=/locale</code> endpoint to execute arbitrary commands. A shell dropper script (dropbbp.sh) is fetched and run, which downloads and installs the botnet malware on the device | <a href="#">CVE-2023-1389</a>  |
| <a href="#">Belsen Group</a> | The Belsen Group is a financially motivated threat actor believed to originate from Yemen, and is known primarily for data extortion and leak-based operations rather than traditional ransomware encryption. The group focuses on breaching organizations, exfiltrating sensitive data, and coercing victims by publicly releasing stolen information on leak sites.                           | <a href="#">CVE-2022-40684</a> |
| <a href="#">DslogdRAT</a>    | DslogdRAT is a new remote access trojan deployed after exploiting a zero-day vulnerability in Ivanti Connect Secure. Installed alongside a web shell, it enables attackers to execute shell commands, transfer files, and proxy traffic. The malware communicates with a remote server via socket, sending system info and awaiting further instructions.                                       | <a href="#">CVE-2025-0282</a>  |
| <a href="#">Flodrix</a>      | Flodrix is a stealthy LeetHozer malware variant that uses self-deletion, artifact removal, and string obfuscation to evade detection and hinder analysis. The malware retrieves C&C instructions while minimizing forensic visibility through advanced anti-analysis techniques.                                                                                                                | <a href="#">CVE-2025-3248</a>  |
| <a href="#">KeyPlug</a>      | Keyplug is a sophisticated backdoor malware primarily associated with targeted intrusion campaigns, enabling long-term remote access to compromised systems. It supports a                                                                                                                                                                                                                      | <a href="#">CVE-2024-23108</a> |

| Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Vulnerabilities Abused         |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
|                               | wide range of capabilities including command execution, file manipulation, credential harvesting, and lateral movement while maintaining a low detection profile.                                                                                                                                                                                                                                                                                                                                                                                                                | <a href="#">CVE-2024-23109</a> |
| <a href="#">Marbled Dust</a>  | Marbled Dust is a threat actor linked to Türkiye, known for highly targeted intrusion campaigns. Its attack chain typically begins with obtaining authenticated access, followed by the exploitation of known vulnerabilities to deepen footholds within victim environments. The group deploys Go-based backdoors to support data exfiltration and remote command execution, and is also notable for DNS hijacking operations and the use of typo-squatted domains to harvest user credentials and maintain long-term access.                                                   | <a href="#">CVE-2025-27920</a> |
| <a href="#">Mimo</a>          | Mimo is a lesser-known but active threat actor observed in targeted intrusion campaigns focused on opportunistic exploitation of exposed services and known vulnerabilities. The group has broadened operations beyond Craft CMS to target Magento e-commerce, Docker hosts, and cloud instances, exploiting software vulnerabilities to deploy an XMRig cryptominer and, in some intrusions, a Go-based ransomware variant tracked as Minus Ransomware.                                                                                                                         | <a href="#">CVE-2025-32432</a> |
| <a href="#">PipeMagic</a>     | PipeMagic is a modular trojan first identified in 2022, enabling code injection into SYSTEM processes and credential theft via LSASS memory dumping. It supports post-exploit actions such as deploying ransomware with randomized file extensions and dropping TOR-linked ransom notes. The trojan is associated with RansomEXX operations and facilitates stealthy lateral movement and data encryption.                                                                                                                                                                       | <a href="#">CVE-2025-24983</a> |
|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2025-29824</a> |
| <a href="#">PolarEdge</a>     | PolarEdge is a botnet targeting Internet of Things (IoT) edge devices (Cisco, ASUS, QNAP, Synology). This botnet employs a stealthy Transport Layer Security (TLS) backdoor, allowing unauthorized access and control over compromised devices.                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2023-20118</a> |
| <a href="#">RESURGE</a>       | RESURGE malware exploits vulnerability in Ivanti Connect Secure devices, to bypass authentication and gain access. After exploitation, it installs a backdoor that enables SSH tunnels for command and control. It alters key system files, avoids integrity checks, and drops a web shell on the Ivanti boot disk. RESURGE also uses encryption to hide its components and activity, making detection and removal more difficult for defenders.                                                                                                                                 | <a href="#">CVE-2025-0282</a>  |
| <a href="#">RedGolf</a>       | RedGolf is a China-linked threat actor known for targeted cyber-espionage campaigns against government, telecommunications, and technology sectors. The group frequently exploits public-facing application vulnerabilities and web shells for initial access, followed by custom backdoors to maintain persistence and conduct intelligence collection. RedGolf's operations emphasize stealth, long-term access, and credential harvesting, aligning with strategic espionage objectives rather than financial gain.                                                           | <a href="#">CVE-2024-23108</a> |
|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2024-23109</a> |
| <a href="#">RondoDox</a>      | RondoDox is an advanced and evolving malware strain that leverages sophisticated evasion techniques such as anti-analysis tactics, XOR-encoded configuration, custom-developed libraries, and a strong persistence strategy.                                                                                                                                                                                                                                                                                                                                                     | <a href="#">CVE-2025-24893</a> |
|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2025-55182</a> |
|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2024-3721</a>  |
|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2024-12856</a> |
|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2023-52163</a> |
| <a href="#">ViciousTrap</a>   | The ViciousTrap threat actor targets edge devices, turning them into honeypots by exploiting vulnerabilities to deploy a shell script that redirects traffic to attacker-controlled infrastructure for network interception. Access is gained through brute-force attacks, authentication bypasses, and vulnerability exploitation, followed by enabling SSH on a custom port and injecting attacker-controlled public keys. Persistence is maintained via NVRAM-stored backdoors, while logging is disabled and no malware is dropped, enabling stealthy and long-term control. | <a href="#">CVE-2023-39780</a> |
|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2023-20118</a> |
|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2021-32030</a> |
| <a href="#">Water Gamayun</a> | Water Gamayun threat actor has been active since at least late 2023 and targets telecommunications and financial sectors. The group employs various techniques including MSC EvilTwin exploitation, sophisticated reconnaissance methods, backdoors like SilentPrism and DarkWisp, as well as information stealers such as Stealc and Rhadamanthys.                                                                                                                                                                                                                              | <a href="#">CVE-2025-24061</a> |
|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2025-24071</a> |
|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2025-26633</a> |

# Tracking CISA KEV – 2025

The Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) catalog is a cornerstone of U.S. national cybersecurity defense, designed to help government agencies and private organizations prioritize threats that pose an immediate and real-world risk. Maintained by CISA, the catalog lists vulnerabilities that are confirmed to be actively exploited by threat actors, meaning they are no longer theoretical weaknesses, but proven entry points used in live attacks. When a vulnerability is added to the KEV catalog, it signals a clear and present danger organizations are expected to treat it as urgent, accelerate patching, and implement mitigations without delay. For U.S. federal agencies, remediation of KEV-listed flaws is mandatory under Binding Operational Directives, and for everyone else, it serves as a trusted benchmark of what attackers are exploiting right now.

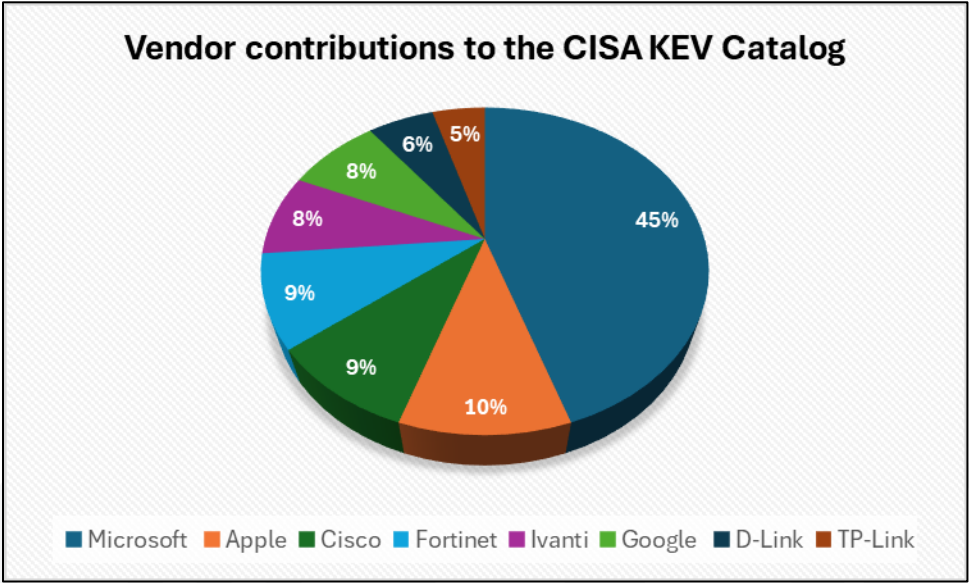
Against this backdrop, 2025 marked a stark escalation in exploitation activity, with 245 vulnerabilities added to the CISA KEV catalog, reflecting an unprecedented pace at which attackers weaponized flaws across diverse technologies. This surge represents a sharp increase compared to 186 vulnerabilities in 2024 and 187 in 2023, underscoring a troubling acceleration in adversary speed and reach. The year was not evenly distributed either March emerged as the most aggressive month with 32 KEV additions, closely followed by October with 31, signaling periods of intense, coordinated exploitation. In contrast, November stood out as the quietest month with just 11 vulnerabilities, offering only a brief lull in an otherwise relentless year. This uneven but upward trend highlights a widening gap between vulnerability disclosure and exploitation, leaving defenders with shrinking response windows and reinforcing that KEV growth is not merely a metric, but a clear warning of an increasingly hostile and unforgiving threat landscape.



*A bar graph illustrating the monthly distribution of CISA KEV additions throughout 2025*

# Vendor-wise contributions to the CISA KEV Catalog

Out of the 246 vulnerabilities added to the CISA KEV catalog, Microsoft emerged as the most impacted vendor, accounting for a striking 39 actively exploited vulnerabilities, underscoring its position as a primary target for threat actors due to its vast enterprise footprint. Apple followed with 9 vulnerabilities, while Cisco and Fortinet each recorded 8, highlighting sustained attacks against core networking and security infrastructure. Google contributed 7 KEV entries, reflecting continued exploitation across widely used platforms, while D-Link (5) and TP-Link (4) rounded out the list, reinforcing how consumer and SMB networking devices remain persistent and attractive targets. Together, this distribution paints a clear picture of where adversaries are concentrating their efforts and where defenders must urgently focus remediation and monitoring.

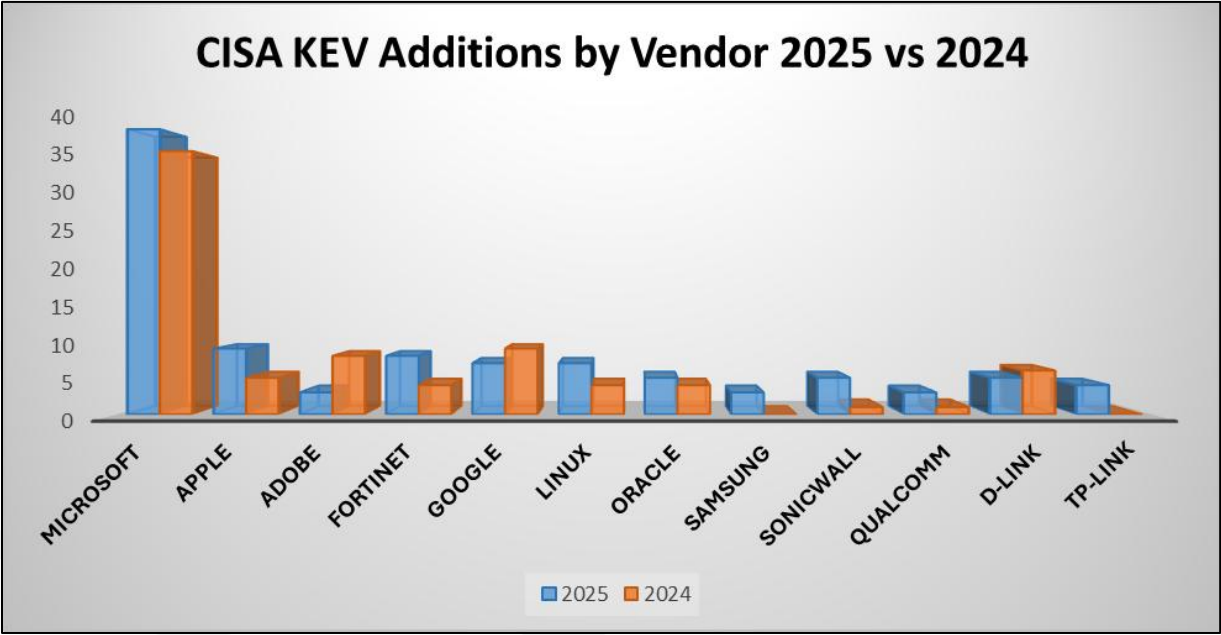


*A pie chart showcasing the distribution of CISA KEV additions by vendor for 2025*

## Comparison between 2025 and 2024

A comparison of vendor vulnerability contributions from 2024 to 2025 reveals a sharply shifting and increasingly urgent security landscape. Microsoft continues to dominate disclosures, rising to 39 in 2025 from 36 in 2024, reinforcing its position as a persistent high-value target for attackers. Apple shows a notable surge from 5 to 9, while Fortinet doubles its count from 4 to 8, highlighting growing pressure on perimeter and network defenses. In contrast, Adobe and Google record declines, though their exposure remains far from negligible.

More concerning is the upward trend among infrastructure and device vendors - Linux, Oracle, SonicWall, Qualcomm, Samsung, and TP-Link, many of which posted zero or minimal numbers previously but show clear growth in 2025. This shift signals expanding attacker focus beyond traditional software targets into firmware, networking gear, and core platforms. If these trajectories persist, 2026 is likely to see even broader exploitation across edge devices and embedded ecosystems, making aggressive patching, asset visibility, and vendor risk prioritization not optional but critical for survival.



*Comparative bar graph of CISA KEV additions by vendor 2025 vs 2024*

# Monthly Breakdown of Actively Exploited Vulnerabilities

In 2025, the cybersecurity landscape was marked by several vulnerabilities that gained significant attention on social media. We are providing a comprehensive overview of these actively exploited vulnerabilities, with a monthly breakdown to highlight their emergence and impact.

## January

2025 opened with a rapidly evolving threat landscape, as January recorded 14 critical vulnerabilities added to CISA KEV catalog. Microsoft led with three vulnerabilities, followed by Mitel with two, while Apple, Ivanti, SonicWall, Fortinet, and Oracle each accounted for one, highlighting early and broad targeting across enterprise and infrastructure technologies. Beyond the KEV additions, CISA issued a warning on critical flaws in Contec CMS8000 patient monitors, underscoring risks to healthcare environments. In a joint advisory with the FBI, authorities also highlighted the active exploitation of Ivanti Cloud Service Appliances as part of an advanced attack chain. Additionally, NETGEAR routers, along with Zyxel and Mitel products, were observed being actively exploited, reinforcing the urgent need for stronger defensive and patching measures at the very start of the year.

| CVE-ID                         | Vendor        | Product                                                | Description                                                                                                                 | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|---------------|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-0282</a>  | Ivanti        | Connect Secure, Policy Secure Neurons for ZTA Gateways | A Stack-based Buffer Overflow vulnerability in Ivanti Connect Secure, Policy Secure, and Neurons for ZTA Gateways           | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-0626</a>  | Contec Health | CMS8000 Patient Monitor                                | A Hidden Functionality vulnerability in Contec Health CMS8000 Patient Monitor                                               | <a href="#">Yes</a>   | No                  | No                  | False |
| <a href="#">CVE-2025-0683</a>  | Contec Health | CMS8000 Patient Monitor                                | An Exposure of Private Personal Information to an Unauthorized Actor vulnerability in Contec Health CMS8000 Patient Monitor | <a href="#">Yes</a>   | No                  | No                  | False |
| <a href="#">CVE-2025-21333</a> | Microsoft     | Windows Hyper-V                                        | An Elevation of Privilege vulnerability in Microsoft Windows Hyper-V NT Kernel Integration VSP                              | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-21334</a> | Microsoft     | Windows Hyper-V                                        | An Elevation of Privilege vulnerability in Microsoft Windows Hyper-V NT Kernel Integration VSP                              | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-21335</a> | Microsoft     | Windows Hyper-V                                        | An Elevation of Privilege vulnerability in Microsoft Windows Hyper-V NT Kernel Integration VSP                              | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-23006</a> | SonicWall     | SMA1000 Appliance Management Console (AMC) and Central | A Deserialization of Untrusted Data vulnerability in the SonicWall SMA1000 AMC and CMC                                      | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor        | Product                                                                                                                                                        | Description                                                                                                               | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
|                                |               | Management Console (CMC)                                                                                                                                       |                                                                                                                           |                       |                     |                     |       |
| <a href="#">CVE-2025-24085</a> | Apple         | Multiple Products                                                                                                                                              | A Use-after-free vulnerability in Apple's Core Media Component                                                            | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-8190</a>  | Ivanti        | Cloud Service Appliance (CSA)                                                                                                                                  | An OS Command Injection vulnerability in Ivanti CSA                                                                       | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-8963</a>  | Ivanti        | Cloud Service Appliance (CSA)                                                                                                                                  | A Path Traversal vulnerability in Ivanti CSA                                                                              | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-9379</a>  | Ivanti        | Cloud Service Appliance (CSA)                                                                                                                                  | A SQL Injection vulnerability in the Ivanti CSA                                                                           | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-9380</a>  | Ivanti        | Cloud Service Appliance (CSA)                                                                                                                                  | A Command Injection vulnerability in the Ivanti CSA                                                                       | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-12248</a> | Contec Health | CMS8000 patient monitor                                                                                                                                        | A Remote Code Execution vulnerability in the Contec Health CMS8000 patient monitor                                        | <a href="#">Yes</a>   | No                  | No                  | False |
| <a href="#">CVE-2024-12686</a> | BeyondTrust   | <ul style="list-style-type: none"> <li>Privileged Remote Access (PRA)</li> <li>Remote Support (RS)</li> </ul>                                                  | An OS Command Injection vulnerability in the BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) solutions | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-12847</a> | NETGEAR       | <ul style="list-style-type: none"> <li>DGN1000</li> <li>DGN2200 v1</li> </ul>                                                                                  | An Authentication Bypass vulnerability in the NETGEAR routers                                                             | <a href="#">Yes</a>   | No                  | No                  | False |
| <a href="#">CVE-2024-40891</a> | Zyxel         | CPE series devices                                                                                                                                             | A Command Injection vulnerability in Zyxel CPE devices                                                                    | <a href="#">Yes</a>   | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2024-41710</a> | Mitel         | <ul style="list-style-type: none"> <li>Mitel 6800 Series</li> <li>Mitel 6900 Series</li> <li>Mitel 6900w Series</li> <li>Mitel 6970 Conference Unit</li> </ul> | A Command Injection vulnerability in Mitel 6800, 6900, and 6900w series SIP phones, including the 6970 Conference Unit    | <a href="#">Yes</a>   | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2024-41713</a> | Mitel         | MiCollab                                                                                                                                                       | A Path Traversal vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab                         | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-50603</a> | Aviatrix      | Network Controller                                                                                                                                             | An Unauthenticated Command Injection vulnerability in the Aviatrix Network Controller                                     | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-52875</a> | GFI Software  | Kerio Control Firewall                                                                                                                                         | A HTTP Response Splitting vulnerability in Kerio Control firewalls                                                        | No                    | No                  | No                  | False |

| CVE-ID                         | Vendor   | Product                                     | Description                                                                                    | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|----------|---------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2024-55550</a> | Mitel    | MiCollab                                    | A Path Traversal vulnerability in the MiCollab server                                          | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-55591</a> | Fortinet | FortiOS and FortiProxy                      | An Authentication Bypass vulnerability in Fortinet FortiOS and FortiProxy                      | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-48365</a> | Qlik     | Sense Enterprise                            | A HTTP Tunneling vulnerability in the Qlik Sense Enterprise                                    | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2022-40684</a> | Fortinet | FortiOS, FortiProxy, and FortiSwitchManager | An Authentication Bypass vulnerability in Fortinet FortiOS, FortiProxy, and FortiSwitchManager | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2020-2883</a>  | Oracle   | WebLogic Server                             | A Deserialization of Untrusted Data vulnerability in the Oracle WebLogic Server                | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2020-11023</a> | jQuery   | jQuery                                      | A Cross-Site Scripting (XSS) vulnerability exists in jQuery                                    | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | True  |

## February

In February 2025, 27 vulnerabilities were added to CISA KEV catalog, impacting vendors such as Microsoft, Palo Alto Networks, Apple, Zyxel, and PostgreSQL. Several of these flaws were exploited as zero-days, while others were actively abused by malware in ongoing campaigns, spanning attack types including authentication bypass, remote code execution, privilege escalation, and command injection across network devices, enterprise applications, and consumer platforms.

| CVE-ID                         | Vendor             | Product                                  | Description                                                                                               | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|--------------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-0108</a>  | Palo Alto Networks | PAN-OS Software                          | An Authentication Bypass vulnerability in the Palo Alto Networks PAN-OS software                          | No                    | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2025-0111</a>  | Palo Alto Networks | PAN-OS Software                          | A File Read vulnerability in the Palo Alto Networks PAN-OS Software                                       | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-0411</a>  | 7-Zip              | 7-Zip                                    | A Mark-of-the-Web Bypass vulnerability in 7-Zip                                                           | Yes                   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-0890</a>  | Zyxel              | CPE Devices                              | A Default Credentials Vulnerability in Zyxel CPE devices                                                  | Yes                   | No                  | No                  | False |
| <a href="#">CVE-2025-0994</a>  | Trimble            | Cityworks                                | Deserialization of Untrusted Data vulnerability in Trimble Cityworks                                      | Yes                   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-1094</a>  | PostgreSQL         | psql                                     | An SQL Injection vulnerability in the PostgreSQL interactive tool psql                                    | Yes                   | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2025-21391</a> | Microsoft          | Windows                                  | A Link Following vulnerability in the Microsoft Windows Storage                                           | Yes                   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-21418</a> | Microsoft          | Windows                                  | A Heap-Based Buffer Overflow vulnerability in the Microsoft Windows Ancillary Function Driver for WinSock | Yes                   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-23209</a> | Craft CMS          | Craft CMS                                | A Code Injection vulnerability in the Craft CMS                                                           | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-24200</a> | Apple              | iOS and iPadOS                           | An Improper Authorization vulnerability in the Apple iPadOS and iOS                                       | Yes                   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24989</a> | Microsoft          | Power Pages                              | An Elevation of Privilege vulnerability in the Microsoft Power Pages                                      | Yes                   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-25181</a> | Advantive          | VeraCore                                 | An SQL Injection vulnerability in Advantive VeraCore                                                      | Yes                   | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2024-20953</a> | Oracle             | Agile Product Lifecycle Management (PLM) | A Deserialization vulnerability in the Oracle Agile Product Lifecycle Management (PLM)                    | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-21413</a> | Microsoft          | Outlook                                  | A Remote Code Execution vulnerability in Microsoft Outlook                                                | Yes                   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-29059</a> | Microsoft          | .NET Framework                           | An Information Disclosure vulnerability in the Microsoft .NET framework                                   | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-38213</a> | Microsoft          | Windows                                  | Security Feature Bypass vulnerability in Microsoft Windows SmartScreen                                    | Yes                   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor     | Product                          | Description                                                                                                            | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2024-40890</a> | Zyxel      | DSL CPE Devices                  | An OS Command Injection vulnerability in the Zyxel DSL CPE series                                                      | Yes                   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-40891</a> | Zyxel      | DSL CPE Devices                  | An OS Command Injection vulnerability in the Zyxel DSL CPE series                                                      | Yes                   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-41710</a> | Mitel      | SIP Phones                       | A Command Injection vulnerability in Mitel 6800, 6900, and 6900w series SIP phones, including the 6970 Conference Unit | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-45195</a> | Apache     | OFBiz                            | A Forced Browsing vulnerability in the Apache OFBiz                                                                    | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-49035</a> | Microsoft  | Partner Center                   | An Improper Privilege Management vulnerability in Partner.Microsoft.com                                                | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-53104</a> | Linux      | Kernel                           | An Out-of-Bounds Write vulnerability in UVCVideo Driver in Linux Kernel                                                | Yes                   | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2024-57727</a> | SimpleHelp | SimpleHelp                       | An Unauthenticated Path Traversal vulnerability in the SimpleHelp Remote Monitoring and Management (RMM) software      | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-34192</a> | Synacor    | Zimbra Collaboration Suite (ZCS) | A Cross-Site Scripting (XSS) vulnerability in Synacor Zimbra Collaboration Suite (ZCS)                                 | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-49103</a> | ownCloud   | owncloud/graphapi                | A Sensitive Information Disclosure vulnerability in the ownCloud owncloud/graphapi                                     | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2022-23748</a> | Audinate   | Dante Discovery                  | A Process Control vulnerability in the Dante Discovery's mDNSResponder.exe                                             | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2020-15069</a> | Sophos     | XG Firewall                      | A Buffer Overflow vulnerability in Sophos XG Firewall could allow remote code execution                                | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2020-29574</a> | Sophos     | Cyberpam OS                      | An SQL Injection vulnerability in the WebAdmin interface of CyberoamOS(CROS)                                           | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2018-9276</a>  | Paessler   | PRTG Network Monitor             | An OS Command Injection vulnerability in Paessler PRTG Network Monitor                                                 | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2018-19410</a> | Paessler   | PRTG Network Monitor             | A Local File Inclusion vulnerability in the Paessler PRTG Network Monitor                                              | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2017-3066</a>  | Adobe      | ColdFusion                       | A Deserialization vulnerability in the Apache BlazeDS library affects Adobe ColdFusion                                 | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |

## March

In March 2025, the cyber threat landscape reached its most active level of the year, marked by a sharp surge in critical vulnerabilities, ransomware activity, and widespread zero-day exploitation. During the month, 32 new vulnerabilities were added to CISA KEV catalog, making it the most actively exploited month in the period. High-impact flaws were identified across major vendors including Edimax, Google, Mozilla, Juniper, VMware, Microsoft and Apple, with particular concern around Chromium and Firefox sandbox escape vulnerabilities that enabled potential privilege escalation on Windows systems.

| CVE-ID                         | Vendor    | Product                      | Description                                                                           | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|-----------|------------------------------|---------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-1316</a>  | Edimax    | IC-7100 IP Camera            | An OS Command Injection vulnerability in the Edimax IC-7100                           | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-2783</a>  | Google    | Chromium Mojo                | Sandbox Escape vulnerability in the Google Chromium Mojo                              | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-2857</a>  | Mozilla   | Firefox                      | Sandbox Escape vulnerability in Mozilla Firefox on Windows systems.                   | False                 | No                  | No                  | False |
| <a href="#">CVE-2025-21590</a> | Juniper   | Junos OS                     | Improper Isolation or Compartmentalization vulnerability in Juniper Junos OS          | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-22224</a> | VMware    | ESXi and Workstation         | A TOCTOU (Time-of-Check Time-of-Use) vulnerability in the VMWare ESXi and Workstation | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-22225</a> | VMware    | ESXi                         | An Arbitrary Write vulnerability in the VMWare ESXi                                   | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-22226</a> | VMware    | ESXi, Workstation and Fusion | An Information Disclosure vulnerability in the VMWare ESXi, Workstation and Fusion    | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24201</a> | Apple     | Multiple Products            | An Out-of-Bounds Write vulnerability in the Apple's WebKit browser engine             | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24472</a> | Fortinet  | FortiOS and FortiProxy       | Authentication Bypass vulnerability in Fortinet FortiOS and FortiProxy                | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24983</a> | Microsoft | Windows                      | A Use-After-Free vulnerability in Microsoft Windows Win32k                            | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24984</a> | Microsoft | Windows                      | An Information Disclosure vulnerability in Microsoft Windows NTFS                     | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24985</a> | Microsoft | Windows                      | An Integer Overflow vulnerability in the Microsoft Windows Fast FAT File System       | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24991</a> | Microsoft | Windows                      | An Out-of-Bounds Read vulnerability in the Microsoft Windows NTFS                     | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24993</a> | Microsoft | Windows                      | A Heap-Based Buffer Overflow vulnerability in the Microsoft Windows NTFS              | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-25181</a> | Advantive | VeraCore                     | An SQL Injection vulnerability in Advantive VeraCore                                  | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-26633</a> | Microsoft | Windows                      | An Improper Neutralization vulnerability in the Microsoft                             | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor             | Product                     | Description                                                                                                         | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|--------------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
|                                |                    |                             | Windows Management Console (MMC)                                                                                    |                       |                     |                     |       |
| <a href="#">CVE-2025-30066</a> | tj-actions         | changed-files GitHub Action | Embedded Malicious Code vulnerability in tj-actions/changed-files GitHub Action                                     | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-30154</a> | reviewdog          | Action-setup GitHub Action  | Embedded Malicious Code vulnerability in the reviewdog action-setup GitHub Action                                   | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-30355</a> | Synapse            | Synapse                     | A Federation Denial-of-Service (DoS) vulnerability via malformed events in Synapse Matrix homeserver implementation | No                    | No                  | No                  | True  |
| <a href="#">CVE-2024-3400</a>  | Palo Alto Networks | PAN-OS Software             | A Command Injection vulnerability in the Palo Alto Networks PAN-OS software                                         | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2024-4345</a>  | Wordpress          | Startklar Elementor plugin  | Arbitrary File Upload vulnerability in the Startklar Elementor Addons WordPress plugin                              | No                    | No                  | No                  | False |
| <a href="#">CVE-2024-4885</a>  | Progress           | WhatsUp Gold                | A Path Traversal vulnerability in the Progress WhatsUp Gold                                                         | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-13159</a> | Ivanti             | Endpoint Manager (EPM)      | Absolute Path Traversal vulnerability in Ivanti Endpoint Manager                                                    | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-13160</a> | Ivanti             | EPM                         | Absolute Path Traversal vulnerability in Ivanti Endpoint Manager                                                    | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-13161</a> | Ivanti             | EPM                         | Absolute Path Traversal vulnerability in Ivanti Endpoint Manager                                                    | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-20439</a> | Cisco              | Smart Licensing Utility     | Use of Static Administrative Credential vulnerability in the Cisco Smart Licensing Utility                          | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-20440</a> | Cisco              | Smart Licensing Utility     | Sensitive Information Disclosure vulnerability in the Cisco Smart Licensing Utility.                                | No                    | No                  | No                  | False |
| <a href="#">CVE-2024-25600</a> | Wordpress          | Bricks Builde               | Arbitrary File Upload vulnerability in the Startklar Elementor Addons WordPress plugin                              | No                    | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2024-27956</a> | Wordpress          | Automatic plugin            | Unauthenticated SQL Injection vulnerability in ValvePress Automatic puglin.                                         | No                    | No                  | No                  | False |
| <a href="#">CVE-2024-48248</a> | NAKIVO             | Backup and Replication      | Absolute Path Traversal vulnerability in the NAKIVO Backup and Replication                                          | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-50302</a> | Linux Foundation   | Linux Kernel                | A Use of Uninitialized Resource vulnerability in the Linux Kernel                                                   | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2024-55591</a> | Fortinet           | FortiOS and FortiProxy      | Authentication Bypass vulnerability in Fortinet FortiOS and FortiProxy                                              | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor                   | Product                                                                                            | Description                                                                                                                                      | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|--------------------------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2024-57040</a> | TP-Link                  | TL-WR845N routers                                                                                  | Use of Hard-coded Credentials vulnerability in the TP-Link TL-WR845N routers                                                                     | <a href="#">Yes</a>   | No                  | No                  | False |
| <a href="#">CVE-2024-57968</a> | Advantive                | VeraCore                                                                                           | An Upload Validation vulnerability in Advantive VeraCore                                                                                         | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-8353</a>  | GiveWP                   | GiveWP                                                                                             | Deserialization of Untrusted Data vulnerability in the GiveWP WordPress plugin                                                                   | No                    | No                  | No                  | False |
| <a href="#">CVE-2023-20118</a> | Cisco                    | RV Series Routers                                                                                  | A Remote Code Execution vulnerability in the Cisco small business router models that enables an attacker to deploy webshell on the target router | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2022-43769</a> | Hitachi Vantara          | Pentaho Business Analytics Server                                                                  | A Special Element Injection vulnerability in Hitachi Vantara Pentaho BA Server                                                                   | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2022-43939</a> | Hitachi Vantara          | Pentaho Business Analytics Server                                                                  | An Authorization Bypass vulnerability in the Hitachi Vantara Pentaho Business Analytics Server                                                   | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2021-20123</a> | Draytek                  | VigorConnect                                                                                       | An Unauthenticated Local File Inclusion vulnerability DownloadFileServlet endpoint of Draytek VigorConnect.                                      | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2021-20124</a> | Draytek                  | VigorConnect                                                                                       | An Unauthenticated Local File Inclusion vulnerability WebServlet endpoint of Draytek VigorConnect                                                | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2021-26855</a> | Microsoft                | Exchange Server                                                                                    | A Remote Code Execution vulnerability in the Microsoft Exchange Server                                                                           | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2021-44228</a> | Apache Server Foundation | Apache Log4j                                                                                       | A Remote Code Execution vulnerability in the Apache Log4j2                                                                                       | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2020-8515</a>  | Draytek                  | <ul style="list-style-type: none"> <li>Vigor 3900</li> <li>Vigor2960</li> <li>Vigor300B</li> </ul> | A Remote Code Execution vulnerability in the DrayTek Vigor3900, Vigor2960, and Vigor300B routers                                                 | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2019-9874</a>  | Sitecore                 | Sitecore CMS and Experience Platform (XP)                                                          | A Deserialization vulnerability in the Sitecore CMS and Experience Platform (XP)                                                                 | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2019-9875</a>  | Sitecore                 | Sitecore CMS and Experience Platform (XP)                                                          | A Deserialization vulnerability in the Sitecore CMS and Experience Platform (XP)                                                                 | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2018-8639</a>  | Microsoft                | Windows                                                                                            | An Improper Resource Shutdown or Release vulnerability in the Microsoft Windows Win32k                                                           | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2017-12637</a> | SAP                      | NetWeaver Application Server Java                                                                  | Directory Traversal vulnerability in the SAP NetWeaver Application Server (AS)                                                                   | Yes                   | No                  | <a href="#">Yes</a> | False |

# April

In April 2025, the threat landscape escalated rapidly as vulnerabilities were not only actively exploited but increasingly weaponized across both enterprise software and consumer devices. During the month, 15 vulnerabilities were added to CISA KEV catalog, spanning a diverse set of technologies. Microsoft, Apple, and Google each accounted for two vulnerabilities, while SonicWall, Ivanti, CrushFTP, and others contributed one each, illustrating how threat actors continued to cast a wide net across multiple technology ecosystems.

| CVE-ID                         | Vendor                         | Product                                                                                                  | Description                                                                                                  | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|--------------------------------|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-0282</a>  | Ivanti                         | <ul style="list-style-type: none"><li>Connect Secure</li><li>Policy Secure</li><li>ZTA Gateway</li></ul> | A Stack-Based Buffer Overflow vulnerability in the Ivanti Connect Secure, Policy Secure and ZTA Gateways     | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-1976</a>  | Brocade Communications Systems | Brocade Fabric OS                                                                                        | A Privilege Escalation via IP Address Validation Flaw in the Brocade Fabric OS                               | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-3102</a>  | Brainstorm Force               | OttoKit WordPress plugin                                                                                 | An Authorization Bypass vulnerability in the OttoKit WordPress plugin (previously known as SureTriggers)     | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-3928</a>  | Commvault                      | Web Server                                                                                               | An Unspecified vulnerability in the Commvault Web Server                                                     | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-22457</a> | Ivanti                         | <ul style="list-style-type: none"><li>Connect Secure</li><li>Policy Secure</li><li>ZTA Gateway</li></ul> | A Stack-Based Buffer Overflow vulnerability in the Ivanti Connect Secure, Policy Secure and ZTA gateways.    | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24054</a> | Microsoft                      | Windows                                                                                                  | A Hash Disclosure Spoofing vulnerability in the Microsoft Windows NTLM                                       | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24813</a> | Apache Software Foundation     | Tomcat                                                                                                   | A Path Equivalence vulnerability in the Apache Tomcat                                                        | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-29824</a> | Microsoft                      | Windows                                                                                                  | A Use-After-Free vulnerability was identified in the Microsoft Windows Common Log File System (CLFS) Driver. | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-30406</a> | Gladinet                       | CentreStack                                                                                              | A Use of Hard-Coded Cryptographic Key vulnerability in Gladinet CentreStack                                  | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-31103</a> | a-blog cms                     | a-blog cms                                                                                               | An Untrusted Data Deserialization vulnerability in a-blog cms.                                               | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-31161</a> | CrushFTP                       | CrushFTP                                                                                                 | An Improper Authentication vulnerability in the CrushFTP                                                     | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-31200</a> | Apple                          | Multiple Products                                                                                        | A Memory Corruption vulnerability in Apple's iOS,                                                            | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor         | Product                                                                       | Description                                                                                                                       | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|----------------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
|                                |                |                                                                               | iPadOS, macOS, and other platforms                                                                                                |                       |                     |                     |       |
| <a href="#">CVE-2025-31201</a> | Apple          | Multiple Products                                                             | An Arbitrary Read and Write vulnerability in Apple iOS, iPadOS, macOS, and other Apple products                                   | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-31324</a> | SAP SE         | SAP NetWeaver Visual Composer                                                 | An Unauthorized File Upload vulnerability in the SAP NetWeaver Visual Composer                                                    | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-32432</a> | Craft CMS      | Craft CMS                                                                     | A Remote Code Execution vulnerability in the Craft CMS                                                                            | <a href="#">Yes</a>   | <a href="#">Yes</a> | No                  | True  |
| <a href="#">CVE-2025-42599</a> | QUALITIA       | Active! mail 6                                                                | A Stack Based Buffer Overflow vulnerability in the Active! Mail 6                                                                 | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-4345</a>  | wshberlin      | Startklar Elementor Addons plugin for WordPress                               | An Arbitrary File Upload vulnerability in the Startklar Elementor addons plugin for WordPress                                     | No                    | No                  | No                  | False |
| <a href="#">CVE-2024-8353</a>  | GiveWP         | Donation Plugin and Fundraising Platform                                      | An Unauthenticated PHP Object Injection vulnerability in GiveWP plugin                                                            | No                    | No                  | No                  | False |
| <a href="#">CVE-2024-11859</a> | ESET           | ESET Products                                                                 | DLL Search Order Hijacking vulnerability in the ESET products                                                                     | No                    | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2024-21762</a> | Fortinet       | FortiOS                                                                       | An Out-of-Bounds Write vulnerability in the Fortinet FortiOS                                                                      | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-25600</a> | Codeer Limited | Bricks Builder                                                                | Unauthenticated Remote Code Execution vulnerability in Codeer Limited Bricks Builder                                              | No                    | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2024-27956</a> | ValvePress     | WordPress Plugin                                                              | Unauthenticated SQL Injection vulnerability in ValvePress Automatic                                                               | No                    | No                  | No                  | False |
| <a href="#">CVE-2024-53150</a> | Google         | Android                                                                       | An Out-of-Bounds vulnerability in the USB sub-component of Kernel                                                                 | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2024-53197</a> | Google         | Android                                                                       | An Out-of-Bounds vulnerability in the USB sub-component of Kernel                                                                 | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2023-27997</a> | Fortinet       | <ul style="list-style-type: none"> <li>FortiOS</li> <li>FortiProxy</li> </ul> | An SSL-VPN Heap-Based Buffer Overflow vulnerability in the Fortinet FortiOS and FortiProxy                                        | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-44221</a> | SonicWall      | SMA 100 Series                                                                | A Post-Authentication OS Command Injection vulnerability has been identified in the SonicWall SMA100 SSL-VPN Management Interface | No                    | No                  | No                  | False |
| <a href="#">CVE-2022-42475</a> | Fortinet       | FortiOS                                                                       | A Heap-Based Buffer Overflow vulnerability in the Fortinet FortiOS                                                                | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor    | Product           | Description                                                                                   | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|-----------|-------------------|-----------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2021-20035</a> | SonicWall | SMA100 Appliances | An OS Command Injection vulnerability in the SonicWall SMA100 Appliances management interface | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2019-0708</a>  | Microsoft | Windows           | A Remote Code Execution vulnerability in the Microsoft Remote Desktop Services                | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2018-0171</a>  | Cisco     | IOS IOS XE        | Remote Code Execution vulnerability in the Cisco IOS and IOS XE software                      | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2017-11882</a> | Microsoft | Office            | A Memory Corruption vulnerability in Microsoft Office                                         | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |



## May

In May 2025, the cyber threat landscape intensified as threat actors aggressively exploited zero-day vulnerabilities at an unprecedented pace. During the month, 25 new vulnerabilities were added to CISA KEV catalog, with an alarming 15 actively exploited as zero-days, reflecting attacker's ability to rapidly weaponize flaws before patches became broadly available. Microsoft accounted for five high-impact vulnerabilities, all exploited prior to disclosure and addressed during May's Patch Tuesday, while Ivanti faced two zero-day flaws leveraged in targeted attacks, likely linked to state-sponsored espionage activity.

| CVE-ID                         | Vendor           | Product                                                                                                         | Description                                                                                    | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-3248</a>  | Langflow         | Langflow                                                                                                        | A Missing Authentication vulnerability in the Langflow                                         | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-4427</a>  | Ivanti           | Endpoint Manager Mobile                                                                                         | An Authentication Bypass vulnerability in the Ivanti Endpoint Manager Mobile                   | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-4428</a>  | Ivanti           | Endpoint Manager Mobile                                                                                         | A Remote Code Execution vulnerability in the Ivanti Endpoint Manager Mobile                    | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-4632</a>  | Samsung          | MagicINFO 9 Server                                                                                              | A Path Traversal vulnerability in the MagicINFO 9 Server                                       | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-4664</a>  | Google           | Chrome                                                                                                          | An Insufficient Policy Loader vulnerability in the Google Chromium Loader                      | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-27007</a> | Brainstorm Force | OttoKit                                                                                                         | An Unauthenticated Privilege Escalation vulnerability in the OttoKit WordPress Plugin          | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-27363</a> | FreeType         | FreeType                                                                                                        | An Out-of-Bounds Write vulnerability in the FreeType font rendering library                    | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-27920</a> | Srimax           | Output Messenger                                                                                                | A Directory Traversal vulnerability in the Srimax Output Messenger                             | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-30397</a> | Microsoft        | Windows                                                                                                         | A Type Confusion vulnerability in the Windows                                                  | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-30400</a> | Microsoft        | Windows                                                                                                         | An Use-After-Free vulnerability in the Microsoft Windows DWM Core Library.                     | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-32701</a> | Microsoft        | Windows                                                                                                         | A Use-After-Free vulnerability in the Windows Common Log File System (CLFS) Driver             | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-32706</a> | Microsoft        | Windows                                                                                                         | A Heap-Based Buffer Overflow vulnerability in the Windows Common Log File System (CLFS) Driver | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-32709</a> | Microsoft        | Windows                                                                                                         | A Use-After-Free vulnerability in the Windows ancillary function driver for WinSock            | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-32756</a> | Fortinet         | <ul style="list-style-type: none"><li>FortiFone</li><li>FortiVoice</li><li>FortiNDR</li><li>FortiMail</li></ul> | A Stack-Based Buffer Overflow vulnerability in Fortinet multiple products                      | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor       | Product                    | Description                                                                                       | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|--------------|----------------------------|---------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-32819</a> | SonicWall    | SMA 100 series             | An Arbitrary File Deletion vulnerability in the SMA 100 series                                    | No                    | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2025-34028</a> | Commvault    | Command Center             | A Path Traversal vulnerability in the Commvault Command Center                                    | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-42999</a> | SAP          | Netweaver                  | A Deserialization vulnerability in the SAP NetWeaver Visual Composer development server           | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-47729</a> | TeleMessage  | TM SGNL                    | A Hidden Functionality vulnerability in the TeleMessage TM SGNL                                   | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-6047</a>  | GeoVision    | Multiple Devices           | An OS Command Injection vulnerability in GeoVision multiple products                              | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-7399</a>  | Samsung      | MagicINFO 9 server         | A Path Traversal vulnerability in the server component of Samsung MagicINFO solution              | No                    | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2024-11120</a> | GeoVision    | Multiple Devices           | An OS Command Injection vulnerability in the GeoVision multiple devices                           | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-11182</a> | MDaemon      | Email Server               | A Cross-Site Scripting (XSS) vulnerability in the MDaemon Email Server                            | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-12987</a> | DrayTek      | Vigor Routers              | An OS Command Injection vulnerability in the DrayTek Vigor routers                                | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-27443</a> | Synacor      | Zimbra Collaboration Suite | A Cross-Site Scripting (XSS) vulnerability in the Zimbra Collaboration Suite (ZCS)                | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-38475</a> | Apache       | HTTP Server                | An Improper Escaping of Output vulnerability in Apache HTTP Server                                | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2024-58136</a> | Yiiframework | Yii                        | An Improper Protection of Alternate Path vulnerability in the PHP web application framework Yii 2 | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2023-20118</a> | Cisco        | RV Series Routers          | A Command Injection vulnerability in the Cisco Small Business RV Series Routers                   | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-38950</a> | ZKTeco       | BioTime                    | A Path Traversal vulnerability in the ZKTeco Biotime                                              | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-44221</a> | SonicWall    | SMA100 Appliances          | An OS Command Injection vulnerability in the SonicWall SMA100 Appliances                          | No                    | No                  | <a href="#">Yes</a> | True  |

## June

In June 2025, organizations faced mounting pressure to reduce patching delays and strengthen their security posture as cyber threats grew increasingly sophisticated and fast-moving. During the month, 20 vulnerabilities were added to CISA KEV catalog. The affected flaws spanned a wide range of technologies including mobile chipsets, CMS platforms, networking devices, and operating systems with confirmed exploitation in products from Qualcomm, ASUS, Craft CMS, Apple, Microsoft, Google, Linux, D-Link, and Fortinet, underscoring sustained targeting of both consumer and enterprise environments by advanced threat actors.

| CVE-ID                         | Vendor                                   | Product               | Description                                                                                      | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|------------------------------------------|-----------------------|--------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-2783</a>  | Google                                   | Chromium Mojo         | A Sandbox Escape vulnerability in the Google Chromium Mojo on Windows                            | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-3248</a>  | Langflow                                 | Langflow              | A Missing Authentication vulnerability in Langflow                                               | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-3935</a>  | ConnectWise                              | ScreenConnect         | An Improper Authentication vulnerability in the ConnectWise ScreenConnect                        | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-4322</a>  | Stylemix Themes                          | Motors theme          | An Unauthenticated Privilege Escalation vulnerability in the Motors theme for WordPress          | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-5419</a>  | Google                                   | Chromium V8           | An Out-of-Bounds Read and Write vulnerability in the Google Chromium V8                          | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-6543</a>  | Citrix                                   | NetScaler ADC/Gateway | A Buffer Overflow vulnerability in the Citrix NetScaler ADC and NetScaler Gateway                | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-21479</a> | Qualcomm                                 | Multiple Chipsets     | An Incorrect Authorization vulnerability in the graphic component of Qualcomm multiple chipsets. | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-21480</a> | Qualcomm                                 | Multiple Chipsets     | An Incorrect Authorization vulnerability in the graphic component of Qualcomm multiple chipsets. | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24016</a> | Wazuh                                    | Wazuh Server          | A Deserialization of Untrusted Data vulnerability in the Wazuh Server                            | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-27038</a> | Qualcomm                                 | Multiple Chipsets     | A Use-after-Free vulnerability in the graphic component of Qualcomm multiple chipsets.           | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-32433</a> | Erlang                                   | Erlang/OTP            | A Missing Authentication for critical vulnerability in the Erlang/OTP SSH Server                 | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-33053</a> | Web Distributed Authoring and Versioning | WebDAV                | External Control of File Name or Path vulnerability in the Web Distributed                       | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor    | Product                                                                      | Description                                                                                                         | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|-----------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
|                                |           |                                                                              | Authoring and Versioning (WebDAV).                                                                                  |                       |                     |                     |       |
| <a href="#">CVE-2025-34037</a> | Linksys   | Multiple Routers                                                             | An OS Command Injection vulnerability in multiple Linksys routers                                                   | Yes                   | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2025-35939</a> | Craft CMS | Craft CMS                                                                    | An External Control of Assumed-Immutable Web Parameter vulnerability in the Craft CMS                               | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-43200</a> | Apple     | Multiple Products                                                            | A Zero-click Logic vulnerability in the Apple multiple products                                                     | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-0769</a>  | D-Link    | DIR-859 Router                                                               | A Path Traversal vulnerability in the D-Link DIR-859 router                                                         | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-3721</a>  | TBK       | <ul style="list-style-type: none"> <li>DVR-4104</li> <li>DVR-4216</li> </ul> | A Command Injection vulnerability in the TBK DVR-4104 and DVR-4216                                                  | No                    | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2024-42009</a> | RoundCube | Webmail                                                                      | A Cross-Site Scripting vulnerability in the RoundCube Webmail                                                       | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2024-54085</a> | AMI       | MegaRAC SPx                                                                  | An Authentication Bypass by Spoofing vulnerability in the AMI MegaRAC SPx in the Redfish Host Interface             | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-56145</a> | Craft CMS | Craft CMS                                                                    | A Code Injection vulnerability in the Craft CMS                                                                     | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2023-0386</a>  | Linux     | Linux Kernel                                                                 | An Improper Ownership Management vulnerability in the Linux Kernel                                                  | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2023-28771</a> | Zyxel     | Multiple Firewalls                                                           | An OS Command Injection vulnerability in the Zyxel Multiple Firewalls                                               | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-33538</a> | TP-Link   | Multiple Routers                                                             | A Command Injection vulnerability in the TP-Link Multiple Routers via the component <b>/userRpm/WlanNetwork Rpm</b> | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-39780</a> | ASUS      | RX-AX55 Routers                                                              | An OS Command Injection vulnerability in the ASUS RX-AX55 routers                                                   | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2021-32030</a> | ASUS      | Routers                                                                      | An Improper Authentication vulnerability in the ASUS Routers                                                        | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2019-6693</a>  | Fortinet  | FortiOS                                                                      | A Use of Hard-Coded Credentials vulnerability in the Fortinet FortiOS                                               | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |

## July

In July 2025, threat actors accelerated their focus on widely used enterprise software, driving a rise in active exploitation and reinforcing the need for rapid vulnerability management across organizations. During the month, 20 vulnerabilities were added to CISA KEV catalog. Microsoft led with three critical flaws, followed by two vulnerabilities in TeleMessage’s TM SGNL platform, reportedly used by a former U.S. National Security Advisor, while Cisco, SysAid, and Google each recorded two high-impact entries, highlighting growing risks across communication, infrastructure, and productivity platforms.

| CVE-ID                         | Vendor      | Product                                                                                                                  | Description                                                                                                         | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-2775</a>  | SysAid      | SysAid On-Prem                                                                                                           | An Improper Restriction of XML External Entity Reference vulnerability in the SysAid On-Prem                        | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-2776</a>  | SysAid      | SysAid On-Prem                                                                                                           | An Improper Restriction of XML External Entity Reference vulnerability in the SysAid On-Prem                        | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-5394</a>  | Bearsthemis | Alone - Charity Multipurpose Non-profit WordPress Theme                                                                  | An Arbitrary File Upload vulnerability in the Alone - Charity Multipurpose Non-profit WordPress Theme for WordPress | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-5777</a>  | Citrix      | NetScaler ADC and Gateway                                                                                                | An Out-of-Bounds Read vulnerability in the Citrix NetScaler ADC and Gateway                                         | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-6554</a>  | Google      | Chromium V8                                                                                                              | A Type Confusion vulnerability in the Google Chromium v8                                                            | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-6558</a>  | Google      | Chromium V8                                                                                                              | An Improper Input Validation vulnerability in the Google Chromium ANGLE and GPU                                     | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-20281</a> | Cisco       | <ul style="list-style-type: none"> <li>Identity Services Engine (ISE)</li> <li>ISE Passive Identity Connector</li> </ul> | An Unauthenticated Remote Code Execution vulnerability in the Cisco ISE and ISE-PIC                                 | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-20282</a> | Cisco       | <ul style="list-style-type: none"> <li>Identity Services Engine (ISE)</li> <li>ISE Passive Identity Connector</li> </ul> | An Arbitrary File Upload vulnerability in the Cisco ISE and ISE-PIC                                                 | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-20337</a> | Cisco       | <ul style="list-style-type: none"> <li>Identity Services Engine (ISE)</li> </ul>                                         | An Unauthenticated Remote Code Execution vulnerability in the Cisco ISE and ISE-PIC                                 | No                    | No                  | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor          | Product                                                                          | Description                                                                                               | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|-----------------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
|                                |                 | <ul style="list-style-type: none"> <li>ISE Passive Identity Connector</li> </ul> |                                                                                                           |                       |                     |                     |       |
| <a href="#">CVE-2025-25257</a> | Fortinet        | FortiWeb                                                                         | A SQL Injection vulnerability in the Fortinet FortiWeb                                                    | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-47812</a> | Wing FTP Server | Wing FTP Server                                                                  | A Remote Code Execution vulnerability in the Wing FTP Server                                              | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-48927</a> | TeleMessage     | TM SGNL                                                                          | An Initialization of a Resource with an Insecure Default vulnerability in the TeleMessage TM SGNL.        | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-48928</a> | TeleMessage     | TM SGNL                                                                          | An Exposure of Core Dump File to an Unauthorized Control Sphere vulnerability in the TeleMessage TM SGNL. | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-49704</a> | Microsoft       | SharePoint                                                                       | A Code Injection vulnerability in Microsoft SharePoint                                                    | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-49706</a> | Microsoft       | SharePoint                                                                       | An Improper Authentication vulnerability in Microsoft SharePoint                                          | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-53770</a> | Microsoft       | SharePoint                                                                       | An Untrusted Data vulnerability in the Microsoft SharePoint                                               | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-53771</a> | Microsoft       | SharePoint                                                                       | An Improper Authentication vulnerability in Microsoft SharePoint server                                   | <a href="#">Yes</a>   | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2025-54309</a> | CrushFTP        | CrushFTP                                                                         | An Unprotected Alternate Channel Vulnerability in the CrushFTP                                            | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-2533</a>  | PaperCut        | NG/MF                                                                            | A Cross-Site Request Forgery vulnerability in the PaperCut NG/MF                                          | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2019-5418</a>  | Rails           | Ruby on Rails                                                                    | A Path Traversal vulnerability in the Rails Ruby on Rails in Action View.                                 | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2019-9621</a>  | Synacor         | Zimbra Collaboration Suite (ZCS)                                                 | A Server-Side Request Forgery (SSRF) vulnerability in the Synacor Zimbra Collaboration Suite (ZCS)        | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2016-10033</a> | PHP             | PHPMailer                                                                        | A Command Injection vulnerability in the PHPMailer                                                        | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2014-3931</a>  | Looking Glass   | Multi-Router Looking Glass (MRLG)                                                | A Buffer Overflow vulnerability in the Multi-Router Looking Glass                                         | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2010-2568</a>  | Microsoft       | Windows                                                                          | A Remote Code Execution vulnerability in Microsoft Windows                                                | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |

## August

In August 2025, the cyber threat landscape continued to evolve rapidly, with 15 vulnerabilities added to the CISA KEV catalog. D-Link and Citrix each accounted for three vulnerabilities, while N-able N-Central and Microsoft recorded two each, highlighting attacker's continued focus on networking infrastructure, IT management tools, and core enterprise technologies.

| CVE-ID                         | Vendor     | Product                                                                              | Description                                                                                                                             | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-7775</a>  | Citrix     | NetScaler                                                                            | A Memory Overflow vulnerability in the Citrix NetScaler                                                                                 | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-8088</a>  | RARLAB     | WinRAR                                                                               | A Path Traversal vulnerability in the RARLAB WinRAR                                                                                     | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-8875</a>  | N-able     | N-Central                                                                            | An Insecure Deserialization vulnerability in N-able N-Central                                                                           | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-8876</a>  | N-able     | N-Central                                                                            | A Command Injection vulnerability in the N-able N-Central                                                                               | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-25256</a> | Fortinet   | FortiSIEM                                                                            | A Remote Code Execution vulnerability in the Fortinet FortiSIEM                                                                         | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-43300</a> | Apple      | <ul style="list-style-type: none"> <li>iOS</li> <li>iPadOS</li> <li>macOS</li> </ul> | An Out-of-Bounds Write vulnerability in the Apple iOS, iPadOS and macOS in the Image I/O framework.                                     | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-48384</a> | Git        | Git                                                                                  | A Link Following vulnerability in the Git                                                                                               | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-54948</a> | TrendMicro | Apex One                                                                             | An OS Command Injection vulnerability in the Trend Micro Apex One Management Console (on-premise)                                       | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-54987</a> | TrendMicro | Apex One                                                                             | Improper Neutralization of Special Elements used in an OS Command vulnerability in Trend Micro Apex One (on-premise) management console | <a href="#">Yes</a>   | No                  | No                  | False |
| <a href="#">CVE-2025-57819</a> | FreePBX    | FreePBX                                                                              | An Authentication Bypass vulnerability in the FreePBX                                                                                   | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-8068</a>  | Citrix     | Session Recording                                                                    | An Improper Privilege Management vulnerability in the Citrix Session Recording                                                          | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-8069</a>  | Citrix     | Session Recording                                                                    | A Deserialization of Untrusted Data vulnerability in the Citrix Session recording                                                       | No                    | No                  | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor    | Product                                                                        | Description                                                                                                             | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|-----------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2024-23692</a> | Rejetto   | HTTP Server                                                                    | An Improper Neutralization of Special Elements Used in a Template Engine vulnerability in the Rejetto HTTP File server. | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-46604</a> | Apache    | ActiveMQ and ActiveMQ Legacy OpenWire Module                                   | A Deserialization of Untrusted Data vulnerability in the Apache ActiveMQ                                                | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2022-40799</a> | D-Link    | DNR-322L                                                                       | A Download of Code Without Integrity Check vulnerability D-Link DNR-322L                                                | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2020-25078</a> | D-Link    | <ul style="list-style-type: none"> <li>DCS-2530L</li> <li>DCS-2670L</li> </ul> | A Remote Password Disclosure vulnerability in the D-Link DCS-2530L and DCS-2670L devices,                               | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2020-25079</a> | D-Link    | <ul style="list-style-type: none"> <li>DCS-2530L</li> <li>DCS-2670L</li> </ul> | A Command Injection vulnerability in the DCS-2530L and DCS-2670L Devices                                                | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2013-3893</a>  | Microsoft | Internet Explorer                                                              | A Resource Management Errors vulnerability in the Microsoft Internet Explorer                                           | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2007-0671</a>  | Microsoft | Office                                                                         | A Remote Code Execution vulnerability in Microsoft Office Excel                                                         | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |

## September

In September 2025, the cybersecurity landscape experienced heightened volatility, driven by increased zero-day activity and intensified exploitation of high-impact vulnerabilities across widely used platforms. During the month, 16 vulnerabilities were added to the CISA KEV catalog, signaling sustained adversary momentum in operationalizing both newly disclosed and previously known flaws.

Cisco and TP-Link accounted for three KEV additions each, highlighting persistent attacker focus on networking and infrastructure components central to enterprise and consumer environments. Additional KEV entries affected vendors such as Sudo, Fortra, Libraesva, Google, Adminer, Linux, Android, Sitecore, and Meta Platforms, reflecting broad exploitation pressure across software, cloud services, and IoT ecosystems.

| CVE-ID                         | Vendor            | Product                                                                        | Description                                                                                                                             | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|-------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-5086</a>  | Dassault Systèmes | DELMIA Apriso                                                                  | Deserialization of Untrusted Data vulnerability in DELMIA Apriso                                                                        | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-5821</a>  | WordPress         | Case Theme User plugin                                                         | An Authentication Bypass vulnerability in the Case Theme User WordPress plugin                                                          | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-9377</a>  | TP-Link           | Multiple Routers                                                               | An OS Command Injection vulnerability in TP-Link Archer C7(EU) and TL-WR841N/ND(MS)                                                     | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-10035</a> | Fortra            | GoAnywhere MFT                                                                 | A Deserialization vulnerability in the License servlet of Fortra's GoAnywhere MFT solution                                              | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-10585</a> | Google            | V8 JavaScript engine                                                           | A Type Confusion vulnerability in the Google Chrome V8 JavaScript Engine and WebAssembly engine.                                        | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-20333</a> | Cisco             | Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense | A Buffer Overflow vulnerability in the Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-20352</a> | Cisco             | <ul style="list-style-type: none"><li>IOS</li><li>IOS XE Software</li></ul>    | A Denial of Service and Remote Code Execution vulnerability in the Cisco IOS and IOS XE software                                        | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-20362</a> | Cisco             | Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense | A Missing Authorization vulnerability in the Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense       | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-32463</a> | Sudo              | Sudo                                                                           | An Inclusion of Functionality from                                                                                                      | No                    | No                  | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor         | Product                                             | Description                                                                                                 | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|----------------|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
|                                |                |                                                     | Untrusted Control Sphere vulnerability in the Sudo                                                          |                       |                     |                     |       |
| <a href="#">CVE-2025-38352</a> | Linux          | Kernel                                              | A Time-of-Check Time-of-Use (TOCTOU) Race Condition vulnerability in the Linux Kernel                       | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-42957</a> | SAP SE         | SAP S/4HANA (private cloud and on-premise editions) | A Command Injection vulnerability in the SAP S/4HANA                                                        | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-48543</a> | Android        | Runtime                                             | A Use-After-Free vulnerability in the Android Runtime that could lead to privilege escalation.              | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-51591</a> | JGM            | Pandoc                                              | A Server-Side Request Forgery vulnerability in the JGM Pandoc                                               | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-53690</a> | Sitecore       | Multiple Products                                   | Deserialization of Untrusted Data vulnerability in Sitecore Multiple Products                               | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-55177</a> | Meta Platforms | WhatsApp                                            | An Incorrect Authorization vulnerability in WhatsApp                                                        | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-59689</a> | Libraesva      | Email Security Gateway                              | A Command Injection vulnerability via a compressed email attachment in the Libraesva Email Security Gateway | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-7344</a>  | Howyar         | Howyar UEFI Application                             | A Remote Code Execution vulnerability in the Howyar Reloader UEFI application                               | No                    | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2024-40766</a> | SonicWall      | SonicOS                                             | An Improper Access Control vulnerability in the SonicWall SonicOS                                           | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-50224</a> | TP-Link        | TL-WR841N                                           | An Authentication Bypass by Spoofing vulnerability in TP-Link TL-WR841N                                     | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2021-21311</a> | Adminer        | Adminer                                             | A Server-Side Request Forgery vulnerability in the Adminer                                                  | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2020-24363</a> | TP-Link        | TL-WA855RE                                          | A Missing Authentication for Critical Function vulnerability in TP-link TL-WA855RE                          | No                    | No                  | <a href="#">Yes</a> | False |

## October

In October 2025, observed as Cybersecurity Awareness Month, the threat landscape highlighted the ongoing need for sustained vigilance and rigorous patch management. During the period, 32 vulnerabilities were added to the CISA KEV catalog, reflecting a marked rise in confirmed in-the-wild exploitation. Microsoft led the additions with eight actively exploited CVEs, while Apple, Kentico, Adobe, and Dassault Systèmes each contributed two entries, signaling continued adversarial focus on operating systems, enterprise platforms, and digital commerce technologies.

Beyond these major vendors, the KEV catalog expanded to include flaws across a broad spectrum of products from SmartBedded Metrobridge, Samsung, Jenkins, Juniper, Oracle, Mozilla, Linux, Synacor, SKYSEA, Grafana Labs, Rapid7, IGEL, Motex, and others, reinforcing that exploitation pressure extended across nearly every layer of the technology ecosystem.

| CVE-ID                         | Vendor            | Product                                    | Description                                                                                            | Exploited as Zero-day | Abused by Malware | CISA KEV            | OSS   |
|--------------------------------|-------------------|--------------------------------------------|--------------------------------------------------------------------------------------------------------|-----------------------|-------------------|---------------------|-------|
| <a href="#">CVE-2025-2746</a>  | Kentico           | Xperience CMS                              | An Authentication Bypass Using an Alternate Path or Channel vulnerability in the Kentico Xperience CMS | No                    | No                | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-2747</a>  | Kentico           | Xperience CMS                              | An Authentication Bypass Using an Alternate Path or Channel vulnerability in the Kentico Xperience CMS | No                    | No                | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-4008</a>  | Smartbedded       | Meteobridge                                | A Command Injection vulnerability in the Smartbedded Meteobridge                                       | No                    | No                | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-5947</a>  | Themeforest       | Service Finder Bookings (WordPress plugin) | An Authentication Bypass vulnerability in the Service Finder Bookings plugin for WordPress             | No                    | No                | No                  | False |
| <a href="#">CVE-2025-6204</a>  | Dassault Systemes | DELMIA Apriso                              | A Code Injection vulnerability in the Dassault Systemes DELMIA Apriso                                  | No                    | No                | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-6205</a>  | Dassault Systemes | DELMIA Apriso                              | A Missing Authorization vulnerability in the Dassault Systemes DELMIA Apriso                           | No                    | No                | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-6264</a>  | Rapid7            | Velociraptor                               | An Incorrect Default Permissions vulnerability in the Rapid7 Velociraptor                              | No                    | No                | No                  | True  |
| <a href="#">CVE-2025-6388</a>  | Theme Spirit      | Spirit Framework (WordPress plugin)        | An Authentication Bypass vulnerability in the Spirit Framework plugin for WordPress                    | No                    | No                | No                  | False |
| <a href="#">CVE-2025-11533</a> | Apsus             | WP Freeio plugin                           | A Privilege Escalation vulnerability in the WP Freeio plugin for WordPress                             | No                    | No                | No                  | False |

| CVE-ID                         | Vendor    | Product                                 | Description                                                                                               | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|-----------|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-21043</a> | Samsung   | Mobile Devices                          | An Out-of-Bounds Write vulnerability in the Samsung                                                       | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-24990</a> | Microsoft | Windows                                 | An Untrusted Pointer Dereference vulnerability in Microsoft Windows                                       | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-27915</a> | Synacor   | Zimbra Collaboration Suite              | A Cross-Site Scripting (XSS) vulnerability in the Zimbra Collaboration                                    | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-33073</a> | Microsoft | Windows                                 | An Improper Access Control vulnerability in the Microsoft Windows SMB Client                              | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-41244</a> | Broadcom  | VMware Aria Operations and VMware Tools | A Privilege Defined with Unsafe Actions vulnerability in Broadcom VMware Aria Operations and VMware Tools | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-47827</a> | IGEL      | IGEL OS                                 | A Use of a Key Past its Expiration Date vulnerability in the IGEL OS                                      | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-54236</a> | Adobe     | Commerce and Magento                    | An Improper Input Validation vulnerability in the Adobe Commerce and Magento                              | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-54253</a> | Adobe     | Experience Manager                      | A Code Execution vulnerability in the Adobe Experience Manager Forms                                      | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-59230</a> | Microsoft | Windows                                 | An Improper Access Control vulnerability in the Microsoft Windows Remote Access Connection Manager        | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-59287</a> | Microsoft | Windows                                 | A Deserialization of Untrusted Data vulnerability in the Microsoft Windows Server Update Service (WSUS).  | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-61882</a> | Oracle    | E-Business Suite                        | An Unspecified vulnerability in Oracle E-Business Suite                                                   | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-61884</a> | Oracle    | E-Business Suite                        | A Server-Side Request Side Forgery vulnerability in the Oracle E-Business Suite                           | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2024-9234</a>  | Wpmet     | GutenKit WordPress plugin               | An Unauthenticated Arbitrary File Upload vulnerability in the GutenKit plugin for WordPress               | No                    | No                  | No                  | False |
| <a href="#">CVE-2024-9707</a>  | ThemeHunk | Hunk Companion                          | A Missing Authorization to Unauthenticated Arbitrary Plugin                                               | No                    | No                  | No                  | False |

| CVE-ID                           | Vendor       | Product                     | Description                                                                          | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|----------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
|                                  |              |                             | installation/activation vulnerability in the Hunk Companion                          |                       |                     |                     |       |
| <a href="#">CVE-2024-11972</a>   | ThemeHunk    | Hunk Companion plugin       | A Remote Code Execution vulnerability in the Hunk Companion WordPress plugin         | No                    | No                  | No                  | False |
| <a href="#">CVE-2024-24893</a>   | XWiki        | XWiki                       | A Remote Code Execution vulnerability in the XWiki                                   | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-43261</a>   | Milesight    | Industrial Cellular Routers | An Information Disclosure vulnerability in the Milesight industrial cellular routers | No                    | No                  | No                  | False |
| <a href="#">CVE-2022-48503</a>   | Apple        | Multiple Products           | An Unspecified vulnerability in Apple multiple products                              | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2021-22555</a>   | Linux        | Kernel                      | An Out-of-Bounds Write vulnerability in the Linux Kernel                             | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2021-43226</a>   | Microsoft    | Windows                     | A Privilege Escalation vulnerability in Microsoft Windows                            | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2021-43798</a>   | Grafana Labs | Grafana                     | A Path Traversal vulnerability in Grafana                                            | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2017-1000353</a> | Jenkins      | Jenkins                     | A Remote Code Execution vulnerability in the Jenkins                                 | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2016-7836</a>    | SKYSEA       | Client View                 | An Improper Authentication vulnerability in the SKYSEA Client View                   | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2015-7755</a>    | Juniper      | ScreenOS                    | An Improper Authentication vulnerability in the Juniper ScreenOS                     | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2014-6278</a>    | GNU          | GNU Bash                    | An OS Command Injection vulnerability in the GNU Bash                                | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2013-3918</a>    | Microsoft    | Windows                     | An Out-of-Bounds Write vulnerability in Microsoft Windows                            | Yes                   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2011-3402</a>    | Microsoft    | Windows                     | A Remote Code Execution vulnerability in Microsoft Windows                           | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2010-3765</a>    | Mozilla      | Multiple Products           | A Remote Code Execution vulnerability in Mozilla multiple products                   | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2010-3962</a>    | Microsoft    | Internet Explorer           | An Uninitialized Memory Corruption vulnerability in the Microsoft Internet Explorer  | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |

# November

In November 2025, adversary activity reflected a clear escalation in both scope and intent, with attackers actively abusing critical infrastructure and widely deployed software components. During the month, 11 vulnerabilities were added to the CISA KEV catalog, impacting vendors such as Fortinet, Gladinet, Microsoft, WatchGuard, Samsung, CWP, Google, Oracle, and OpenPLC, highlighting sustained pressure across enterprise, cloud and application-layer environments.

Beyond the KEV additions, exploitation extended to legacy and third-party ecosystems, with active attacks observed against outdated ASUS routers, the Noo JobMonster WordPress theme, the Sneeit Framework plugin, and even patched versions of 7-Zip, reinforcing how attackers continued to capitalize on delayed patching and residual exposure.

| CVE-ID                         | Vendor                     | Product                      | Description                                                                                         | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|----------------------------|------------------------------|-----------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-2492</a>  | Asus                       | Routers                      | An Improper Authentication vulnerability in the ASUS AiCloud                                        | No                    | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2025-5397</a>  | Noo                        | JobMonster (WordPress Theme) | An Authentication Bypass vulnerability in the JobMonster WordPress theme                            | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-6389</a>  | Sneeit                     | Sneeit Framework             | An Unauthenticated Remote Code Execution vulnerability in the Sneeit Framework plugin for WordPress | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-9242</a>  | WatchGuard                 | Firebox                      | An Out-of-Bounds Write vulnerability in the WatchGuard Firebox                                      | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-9491</a>  | Microsoft                  | Windows                      | A Remote Code Execution vulnerability in the Microsoft Windows LNK File UI Misrepresentation.       | <a href="#">Yes</a>   | <a href="#">Yes</a> | No                  | False |
| <a href="#">CVE-2025-11001</a> | 7-Zip                      | 7-Zip                        | A File Parsing Directory Traversal Remote Code Execution vulnerability in 7-ZIP                     | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-11371</a> | Gladinet                   | CentreStack and Triofox      | A Local File Inclusion vulnerability in the Gladinet CentreStack and TrioFox                        | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-11833</a> | WordPress plugin developer | Post SMTP WordPress Plugin   | A Missing Authorization vulnerability in the Post SMTP WordPress Plugin                             | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-12480</a> | Gladinet                   | Triofox                      | An Improper Access Control vulnerability in the Gladinet Triofox                                    | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-13223</a> | Google                     | Chromium V8                  | A Type Confusion vulnerability in the Google Chromium V8                                            | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-21042</a> | Samsung                    | Mobile Devices               | An Out-of-Bounds Write vulnerability in the Samsung mobile devices in the libimagecodec.quram.so.   | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor    | Product           | Description                                                                                  | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|-----------|-------------------|----------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-48703</a> | CWP       | Control Web Panel | An OS Command Injection vulnerability in the Control Web Panel                               | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-58034</a> | Fortinet  | FortiWeb          | An OS Command Injection vulnerability in the Fortinet FortiWeb                               | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-61757</a> | Oracle    | Fusion Middleware | A Missing Authentication for Critical Function vulnerability in the Oracle Fusion Middleware | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-62215</a> | Microsoft | Windows           | A Race Condition vulnerability in Microsoft Windows                                          | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-64446</a> | Fortinet  | FortiWeb          | A Path Traversal Vulnerability in the Fortinet FortiWeb                                      | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2021-26829</a> | OpenPLC   | ScadaBR           | A Cross-Site Scripting Vulnerability in the OpenPLC ScadaBR via <b>system_settings.shtm</b>  | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |



## December

In December 2025, the threat landscape reflected a hardened exploitation environment, with high-impact vulnerabilities being swiftly weaponized and integrated into active attack chains. Over the course of the month, 20 flaws were added to the CISA KEV catalog, impacting major vendors including Microsoft, Google, Apple, Fortinet, and ASUS. The wide scope of affected products underscored sustained adversarial focus on both consumer and enterprise technologies that form the backbone of global digital infrastructure.

A notable standout was a Meta React Server Components vulnerability, which saw active exploitation by multiple threat actors and was assessed to represent a persistent long-term risk due to its extensive adoption and deep integration in modern web applications.

| CVE-ID                         | Vendor                     | Product                                                                                                        | Description                                                                                                                                       | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-6218</a>  | RARLAB                     | WinRAR                                                                                                         | A Path Traversal vulnerability in RARLAB WinRAR                                                                                                   | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-8110</a>  | Gogs                       | Gogs Self-Hosted Git Service                                                                                   | An Improper Symbolic link handling vulnerability in Gogs Git service                                                                              | <a href="#">Yes</a>   | No                  | No                  | True  |
| <a href="#">CVE-2025-8489</a>  | WordPress plugin ecosystem | King Addons for Elementor – Free Elements, Widgets, Templates, and Features for Elementor plugin for WordPress | A Privilege Escalation vulnerability in the King Addons for Elementor - Free Elements, Templates, and Features for Elementor plugin for WordPress | No                    | No                  | No                  | False |
| <a href="#">CVE-2025-14174</a> | Google                     | Chromium                                                                                                       | An Out of Bounds Memory Access vulnerability in the Google Chromium                                                                               | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-14611</a> | Gladinet                   | CentreStack and Triofox                                                                                        | A Hard Coded Cryptographic vulnerability in Gladinet CentreStack and Triofox                                                                      | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-14733</a> | WatchGuard                 | Firebox                                                                                                        | An Out of Bounds Write vulnerability in the WatchGuard Firebox in the OS iked process.                                                            | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-14847</a> | MongoDB                    | MongoDB and MongoDB Server                                                                                     | An Improper Handling of Length Parameter Inconsistency vulnerability in MongoDB and MongoDB Server                                                | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-20393</a> | Cisco                      | Multiple Products                                                                                              | An Improper Input Validation vulnerability in Cisco Multiple Products                                                                             | <a href="#">Yes</a>   | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-40602</a> | SonicWall                  | SMA1000 appliance                                                                                              | A Missing Authorization vulnerability in SonicWall SMA1000                                                                                        | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-43529</a> | Apple                      | Multiple Products                                                                                              | A Use-After-Free WebKit vulnerability in Apple Multiple products                                                                                  | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |

| CVE-ID                         | Vendor          | Product                                                                                                                     | Description                                                                                                                     | Exploited as Zero-day | Abused by Malware   | CISA KEV            | OSS   |
|--------------------------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|---------------------|-------|
| <a href="#">CVE-2025-48572</a> | Android         | Framework                                                                                                                   | A Privilege Escalation vulnerability in the Android Framework                                                                   | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-48633</a> | Android         | Framework                                                                                                                   | An Information Disclosure vulnerability in the Android Framework                                                                | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-55182</a> | Meta            | React Server Components                                                                                                     | A Remote Code Execution vulnerability Meta React Server Components                                                              | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-58360</a> | OSGeo           | GeoServer                                                                                                                   | An Improper Restriction of XML External Entity Reference vulnerability in the OSGeo GeoServer                                   | No                    | No                  | <a href="#">Yes</a> | True  |
| <a href="#">CVE-2025-59374</a> | ASUS            | Live Update                                                                                                                 | An Embedded Malicious Code vulnerability in the ASUS Live Update                                                                | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-59718</a> | Fortinet        | <ul style="list-style-type: none"> <li>FortiOS</li> <li>FortiSwitch Master</li> <li>FortiProxy</li> <li>FortiWeb</li> </ul> | An Improper Verification of Cryptographic Signature vulnerability in Fortinet multiple products                                 | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-62221</a> | Microsoft       | Windows                                                                                                                     | A Use After Free vulnerability in Microsoft Windows                                                                             | <a href="#">Yes</a>   | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2025-66644</a> | Array Networks  | ArrayOS AG                                                                                                                  | An OS Command Injection vulnerability in the Array Networks ArrayOS AG                                                          | No                    | No                  | <a href="#">Yes</a> | False |
| <a href="#">CVE-2023-52163</a> | Digiever        | DS-2105 Pro                                                                                                                 | A Missing Authorization vulnerability in Digiever DS-2105 Pro allows for command injection via <b><i>time_tzsetup.cgi</i></b> . | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2022-37055</a> | D-Link          | Routers                                                                                                                     | A Buffer Overflow vulnerability in the D-Link Routers                                                                           | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2021-26828</a> | OpenPLC         | ScadaBR                                                                                                                     | An Unrestricted Upload of File with Dangerous Type vulnerability in the OpenPLC ScadaBR                                         | No                    | <a href="#">Yes</a> | <a href="#">Yes</a> | False |
| <a href="#">CVE-2018-4063</a>  | Sierra Wireless | AirLink ALEOS                                                                                                               | An Unrestricted Upload of File with Dangerous Type vulnerability in Sierra Wireless AirLink ALEOS                               | No                    | No                  | <a href="#">Yes</a> | False |

## Conclusion: Preparing for What Comes Next

The cybersecurity events of 2025 make it clear that reactive models are no longer sufficient in an environment where vulnerabilities are exploited within hours and trust chains are routinely abused. As attackers continue to evolve their tactics across software supply chains, identities, and cloud-native ecosystems, organizations must move beyond severity-based risk assessments toward exploitation-aware decision-making.

Looking ahead to 2026, success will depend on how quickly defenders can identify which vulnerabilities truly matter, understand who is exploiting them, and act before exploitation becomes widespread. Loginsoft Vulnerability Intelligence enables this shift by continuously tracking and monitoring exploited vulnerabilities, emerging malware, and active threat actors, translating raw threat data into actionable intelligence. By adopting a threat-informed approach, organizations can move into 2026 with clarity, confidence, and a measurable defensive advantage.



## Sources Cited

1. <https://www.cisa.gov/news-events/alerts/2025/01/08/cisa-adds-one-vulnerability-kev-catalog>
2. <https://www.cisa.gov/news-events/alerts/2025/01/29/cisa-adds-one-known-exploited-vulnerability-catalog>
3. <https://www.cisa.gov/news-events/alerts/2025/02/11/cisa-adds-four-known-exploited-vulnerabilities-catalog>
4. <https://www.cisa.gov/news-events/alerts/2025/02/20/cisa-adds-two-known-exploited-vulnerabilities-catalog>
5. <https://www.cisa.gov/news-events/alerts/2025/03/18/cisa-adds-two-known-exploited-vulnerabilities-catalog>
6. <https://www.cisa.gov/news-events/alerts/2025/03/19/cisa-adds-three-known-exploited-vulnerabilities-catalog>
7. <https://www.cisa.gov/news-events/alerts/2025/04/08/cisa-adds-two-known-exploited-vulnerabilities-catalog>
8. <https://www.cisa.gov/news-events/alerts/2025/04/28/cisa-adds-three-known-exploited-vulnerabilities-catalog>
9. <https://www.cisa.gov/news-events/alerts/2025/05/13/cisa-adds-five-known-exploited-vulnerabilities-catalog>
10. <https://www.cisa.gov/news-events/alerts/2025/05/19/cisa-adds-six-known-exploited-vulnerabilities-catalog>
11. <https://www.cisa.gov/news-events/alerts/2025/06/02/cisa-adds-five-known-exploited-vulnerabilities-catalog>
12. <https://www.cisa.gov/news-events/alerts/2025/06/03/cisa-adds-three-known-exploited-vulnerabilities-catalog>
13. <https://www.cisa.gov/news-events/alerts/2025/07/22/cisa-adds-four-known-exploited-vulnerabilities-catalog>
14. <https://www.cisa.gov/news-events/alerts/2025/07/28/cisa-adds-three-known-exploited-vulnerabilities-catalog>
15. <https://www.cisa.gov/news-events/alerts/2025/08/12/cisa-adds-three-known-exploited-vulnerabilities-catalog>
16. <https://www.cisa.gov/news-events/alerts/2025/08/18/cisa-adds-one-known-exploited-vulnerability-catalog>
17. <https://www.cisa.gov/news-events/alerts/2025/09/03/cisa-adds-two-known-exploited-vulnerabilities-catalog>
18. <https://www.cisa.gov/news-events/alerts/2025/09/29/cisa-adds-five-known-exploited-vulnerabilities-catalog>
19. <https://www.cisa.gov/news-events/alerts/2025/10/20/cisa-adds-five-known-exploited-vulnerabilities-catalog>
20. <https://www.cisa.gov/news-events/alerts/2025/10/28/cisa-adds-two-known-exploited-vulnerabilities-catalog>
21. <https://www.cisa.gov/news-events/alerts/2025/11/12/cisa-adds-three-known-exploited-vulnerabilities-catalog>

22. <https://www.cisa.gov/news-events/alerts/2025/11/04/cisa-adds-two-known-exploited-vulnerabilities-catalog>
23. <https://www.cisa.gov/news-events/alerts/2025/12/09/cisa-adds-two-known-exploited-vulnerabilities-catalog>
24. <https://www.cisa.gov/news-events/alerts/2025/12/15/cisa-adds-two-known-exploited-vulnerabilities-catalog>
25. [https://www.trendmicro.com/en\\_us/research/25/f/langflow-vulnerability-flodric-botnet.html](https://www.trendmicro.com/en_us/research/25/f/langflow-vulnerability-flodric-botnet.html)
26. <https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/>
27. <https://asec.ahnlab.com/en/85000/>
28. [https://www.trendmicro.com/en\\_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html](https://www.trendmicro.com/en_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html)
29. <https://blog.talosintelligence.com/uat-6382-exploits-cityworks-vulnerability/>
30. <https://blog.alphahunt.io/vmware-vulnerabilities-apt29-apt41-and-apt28s-exploitation-tactics/>
31. <https://blogs.jpcert.or.jp/en/2025/04/dslogdrat.html>
32. [https://www.trendmicro.com/en\\_us/research/25/j/rondodox.html](https://www.trendmicro.com/en_us/research/25/j/rondodox.html)
33. <https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/>



# About LOVI

In today's rapidly evolving digital ecosystem, threat actors continuously discover new ways to exploit vulnerabilities across software, hardware, and open-source ecosystems, turning even minor flaws into major security incidents. LOVI (Loginsoft Vulnerability Intelligence) stands as a powerful, research-driven solution designed to transform raw vulnerability data into real-time, actionable intelligence. As a Research-as-a-Service (RaaS) platform, LOVI delivers deep technical insights, contextual risk assessments, and enriched CVE intelligence that enable organizations to stay one step ahead of attackers and make faster, smarter security decisions.

The platform centralizes trusted sources such as the CISA Known Exploited Vulnerabilities (KEV) Catalog and the National Vulnerability Database (NVD), while automated, customizable alerts notify teams the moment high-impact vulnerabilities emerge. Through AI-powered risk prioritization and lifecycle tracking, LOVI reduces alert fatigue, accelerates remediation, and delivers a strategic advantage in securing modern, interconnected digital environments.

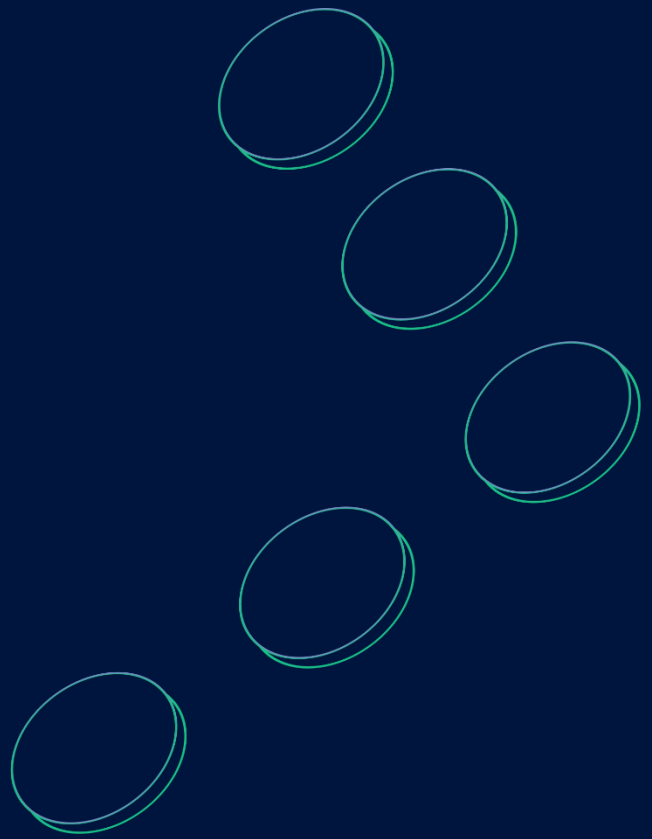
LOVI also delivers dedicated intelligence by tracking trending vulnerabilities across all the platforms, analyzing dependency risks, and correlating CVEs across widely used libraries and frameworks. By enriching OSS-related findings with exploitability data, EPSS scores, and real-world attack patterns, teams gain clear visibility into supply chain risks and third-party exposure.

## Loginsoft Vulnerability Intelligence

**See threats sooner**

**Prioritize smarter**

**Secure with confidence**



# About Loginsoft

**Loginsoft** is a specialized cybersecurity services company providing customized solutions to Cybersecurity companies and enterprises since 2005. Headquartered in Virginia, USA, Loginsoft provides end-to-end cybersecurity capabilities, including threat intelligence, threat hunting, vulnerability and zero-day research, open-source software risk analysis, software supply chain security, security & threat intelligence integrations and security advisory services. The company is recognized for its deep expertise in vulnerability intelligence, producing enriched vulnerability metadata and developing accurate detection signatures using the MITRE OVAL language. Backed by flexible delivery models onsite, offsite, and offshore and a strong emphasis on continuous research and innovation, Loginsoft enables organizations to proactively manage cyber risk and maintain long-term security resilience.



Visit [www.loginsoft.com](http://www.loginsoft.com)



## USA Office

4437 Brookfield  
Corporate Drive, Suite 101  
Chantilly, VA USA 20151



## Canada Office

7-7003 Steeles Ave W,  
Toronto, ON M9W 0A2,  
Canada



## India Office

1-63-5-8B, Kavuri Hills,  
Jubilee Hills, Hyderabad-  
500033