loginsoft

Monthly Report

# Threat & Vulnerabilities Report – August 2025

# Executive Summary

The cyber threat landscape continued to evolve rapidly, with critical flaws surfacing across widely used enterprise and consumer technologies. CISA's Known Exploited Vulnerabilities (KEV) catalog remained a key indicator of active exploitation trends, highlighting where attackers are striking most.

A total of 15 vulnerabilities entered the KEV catalog this month, with D-Link and Citrix each accounting for three and N-able N-Central and Microsoft accounting for two each, reflecting how attackers continue to target technologies across networking, IT management, and enterprise ecosystems.

Ransomware activity spiked this month, with Qilin, Akira, and Safepay leading the charge. The education, finance, and manufacturing sectors were hit the hardest, with attackers leveraging known unpatched vulnerabilities to break into critical systems.

# Actively Exploited Vulnerabilities

| CVE-ID | Vendor | Product | Description | Exploited as Zero-day | Abused by Malware | CISA KEV | OSS |
|---|---|---|---|---|---|---|---|
| CVE-2025-7775 | Citrix | NetScaler | A Memory Overflow Vulnerability in the Citrix NetScaler enables remote code execution or denial of service. | Yes | No | Yes | False |
| CVE-2025-8088 | RARLAB | WinRAR | A Path Traversal Vulnerability in the RARLAB WinRAR that enables attackers to execute arbitrary code by crafting malicious archive files. | Yes | No | Yes | False |
| CVE-2025-8875 | N-able | N-Central | An Insecure Deserialization Vulnerability in N-able N-Central could lead to command execution. | Yes | No | Yes | False |
| CVE-2025-8876 | N-able | N-Central | A Command Injection Vulnerability in the N-able N-Central via improper sanitization of user input. | Yes | No | Yes | False |
| CVE-2025-25256 | Fortinet | FortiSIEM | A Remote Code Execution Vulnerability in the Fortinet FortiSIEM enables an unauthenticated attacker to execute commands via crafted CLI requests. | No | No | No | False |
| CVE-2025-43300 | Apple | • iOS<br>• iPadOS<br>• macOS | An Out-of-Bounds Write Vulnerability in the Apple iOS, iPadOS and macOS in the Image I/O framework. | Yes | No | Yes | False |
| CVE-2025-48384 | Git | Git | A Link Following Vulnerability in the Git that stems from Git's | No | No | Yes | False |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | inconsistent handling of carriage return characters in configuration files. | | | | |
| CVE-2025-54948 | TrendMicro | Apex One | An OS Command Injection Vulnerability in the Trend Micro Apex One Management Console (on-premise) that enables a pre-authenticated remote attacker to upload malicious codes on affected installations. | Yes | No | Yes | False |
| CVE-2025-54987 | TrendMicro | Apex One | Improper Neutralization of Special Elements used in an OS Command Vulnerability in Trend Micro Apex One (on-premise) management console that enables a remote attacker to execute malicious commands on affected installations. | Yes | No | No | False |
| CVE-2025-57819 | FreePBX | FreePBX | An Authentication Bypass Vulnerability in the FreePBX that can lead to database manipulation and remote code execution and SQL injection. | Yes | No | Yes | False |
| CVE-2024-8068 | Citrix | Session Recording | An Improper Privilege Management Vulnerability in the Citrix Session Recording that enables privilege escalation to ***NetworkService*** Account access. | No | No | Yes | False |
| CVE-2024-8069 | Citrix | Session Recording | A Deserialization of Untrusted Data Vulnerability in the Citrix Session recording that enables limited remote code execution with privilege of a ***NetworkService*** Account access. | No | No | Yes | False |
| CVE-2024-23692 | Rejetto | HTTP Server | An Improper Neutralization of Special Elements Used in a Template Engine Vulnerability in the Rejetto HTTP File server. | No | Yes | Yes | False |
| CVE-2023-46604 | Apache | ActiveMQ and ActiveMQ Legacy OpenWire Module | A Deserialization of Untrusted Data Vulnerability in the Apache ActiveMQ Q enables a remote attacker with network access to run arbitrary shell commands. | No | Yes | Yes | True |
| CVE-2022-40799 | D-Link | DNR-322L | A Download of Code Without Integrity Check Vulnerability D-Link DNR- | No | No | Yes | False |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | 322L that enables an authenticated attacker to execute OS level commands on the device. | | | | |
| CVE-2020-25078 | D-Link | • DCS-2530L<br>• DCS-2670L | A Remote Password Disclosure Vulnerability in the D-Link DCS-2530L and DCS-2670L devices, via ***/config/getuser endpoint***. | No | Yes | Yes | False |
| CVE-2020-25079 | D-Link | • DCS-2530L<br>• DCS-2670L | A Command Injection Vulnerability in the DCS-2530L and DCS-2670L Devices through the ***cgi-bin/ddns_enc.cgi***. | No | No | Yes | False |
| CVE-2013-3893 | Microsoft | Internet Explorer | A Resource Management Errors Vulnerability in the Microsoft Internet Explorer that allows for remote code execution. | No | Yes | Yes | False |
| CVE-2007-0671 | Microsoft | Office | A Remote Code Execution Vulnerability in Microsoft Office Excel that could be exploited when a specially crafted Excel file is opened. | No | No | Yes | False |

# Ransomware Insights for August

The Ransomware insights were captured from various data leak sites of respective ransomware. This insight helps us to understand which industries and countries were targeted the most

| Ransomware | Description | No.of Affected Organizations for August | Targeted Industries | Vulnerabilities Abused Most |
|---|---|---|---|---|
| **Qilin** | The Qilin ransomware has been in existence since August 2022, also recognized as Agenda, and has posed a substantial threat. Employing Rust and Go programming languages, this ransomware group executes intricate and elusive attack strategies. It's developed in Rust and identified as Ransom.Win32.AGENDA.THIAFBB, was discovered. Remarkably, this ransomware initially scripted in Go language was notorious for its focus on healthcare and education sectors, particularly in nations such as Thailand and Indonesia. | 82 | • Education<br>• Healthcare | • CVE-2025-31324<br>• CVE-2024-21762<br>• CVE-2024-55591<br>• CVE-2023-27532 |
| **Akira** | Akira ransomware underscored a critical security vulnerability linked to the lack of Multi-Factor Authentication (MFA). The nations | 56 | • Education<br>• Manufacture<br>• Finance | • CVE-2020-1472<br>• CVE-2020-3259 |

| | | | | |
|---|---|---|---|---|
| | experiencing the fallout encompass the United States, the United Kingdom, Canada, Australia, and South Korea. The repercussions are noteworthy, especially within pivotal domains like Services and Goods, Manufacturing, Education, and Finance. | | | |
| **Safepay** | SafePay is a newly emerging ransomware strain believed to be derived from leaked LockBit source code, distinguished by its ransom note titled "readme_safepay.txt" and encrypted file extensions labeled ".safepay." While bearing similarities to LockBit, SafePay's refined approach establishes it as a formidable new player in the ransomware landscape. It employs a two-phase attack strategy involving initial system infiltration followed by data encryption, often using anti-detection mechanisms to evade security measures. Linked to the LockBit ransomware builder, SafePay is suspected to involve experienced cybercriminals in its creation and deployment. The ransomware primarily targets payment processors and banks, posing a significant threat to financial institutions. With at least 22 victims reported so far, SafePay's sophisticated techniques for spreading and exfiltrating data underscore its potency and highlight the challenges of mitigating its impact. | 29 | • Education<br>• Finance<br>• Agriculture<br>• Manufacturing<br>• Healthcare<br>• Logistic | Unknown |
| **DragonForce** | 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 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 | 27 | • Government entities<br>• Infrastructure sectors | • CVE-2024-57727<br>• CVE-2024-57728<br>• CVE-2024-57726<br>• CVE-2022-26134 |

| | | | | |
|---|---|---|---|---|
| | has also threatened to release stolen information on dark web leak sites to pressure victims into paying ransoms. | | | |
| **Inc Ransom** | Inc. ransomware, which emerged in June 2023, spread through spear-phishing emails and targeted vulnerable services, such as the exploitation of **CVE-2023-3519** in Citrix NetScaler. Our observations indicate that Inc. ransomware has deliberately targeted a range of sectors, including healthcare, education, and government entities. This ransomware operates as a multi-extortion scheme, involving the theft of victim data and threats to release the data online unless the victim complies with their demands. | 21 | • Education<br>• Healthcare<br>• Government sectors | • CVE-2023-3519 |
| **Play** | The Play ransomware group, also identified as Balloonfly and PlayCrypt, has significantly impacted businesses and critical infrastructure across North America, South America and Europe regions. With a primary focus on telecommunications, the group has extended its reach to healthcare, technology and media industries. It was observed that the group focused on managed service providers (MSPs) globally, using remote monitoring and management (RMM) tools to infiltrate customer systems. Their campaigns involve custom tools like "Grixba" and "VSS Copying Tool" written in .NET. Interestingly, Play ransomware affiliates prefer email communication for negotiations and do not provide Tor negotiation page links in ransom notes on compromised systems. | 20 | • Healthcare<br>• Media<br>• Technology<br>• Telecommunication | • CVE-2022-41040<br>• CVE-2022-41080<br>• CVE-2022-41082<br>• CVE-2021-34523<br>• CVE-2020-12812<br>• CVE-2018-13379 |
| **Lynx** | Lynx ransomware, active since mid-2024, is a sophisticated malware operating under a ransomware-as-a-service (RaaS) model, claiming over 20 victims across various industries. It employs single and double extortion tactics, encrypting critical files with a ".lynx" extension and threatening to leak data if ransoms are unpaid, while also deleting backups like shadow copies to hinder recovery. Notably, Lynx has targeted organizations in the United States, United Kingdom, | 13 | • Finance<br>• Retail<br>• Real Estate<br>• Manufacture<br>• Construction<br>• Logistic | Unknown |

| | | | | |
|---|---|---|---|---|
| | Canada, Guatemala, and Australia, with a significant attack on Romania's Electrica Group, demonstrating its capacity to disrupt critical infrastructure. The ransomware employs a hybrid encryption method, using AES for file encryption and RSA for key protection, and directs victims to Tor communication channels for ransom negotiations. Key features include targeting specific directories for encryption, terminating processes, encrypting network drives, escalating privileges, and altering system settings, such as background images. By employing these sophisticated techniques, Lynx continues to pose a serious threat to industries worldwide. | | | |
| **Rhysida** | Rhysida ransomware has a new variant that provides Ransomware-as-a-service (RaaS). As of 2023, approximately 50 victims have been identified, targeting the Education, Healthcare, Manufacturing, Information Technology and Government sectors. The deployment of Rhysida involves various methods, including the use of Cobalt Strike or a similar framework, as well as phishing campaigns. Notably, we have observed the threat actor exploiting Zerologon's (**CVE-2020-1472**) vulnerability, a critical elevation of privileges flaw in Microsoft's Netlogon Remote Protocol. Upon gaining network access, the Rhysida gang employs Living off the Land Binaries (LoLBins) techniques to execute malicious activities discreetly and avoid detection. | 6 | • Education<br>• Healthcare<br>• Manufacturing<br>• Information Technology<br>• Government sectors | • CVE-2020-1472 |
| **Medusa** | Emerging in 2019, the Medusa ransomware operates on a ransomware-as-a-service (RaaS) model and has been observed infecting and encrypting systems in various sectors, notably focusing on the healthcare sector. Attackers typically gain initial access through brute-force assaults on Remote Desktop Protocol (RDP), exploiting leaked RDP credentials, or employing | 4 | • Healthcare<br>• Finance<br>• Technology<br>• Manufacturing | • CVE-2023-0669<br>• CVE-2023-27350<br>• CVE-2023-27351<br>• CVE-2023-34362<br>• CVE-2023-47246<br>• CVE-2022-2295 |

| | | | | |
|---|---|---|---|---|
| | spear-phishing tactics to acquire user credentials. Notably, ransomware affiliates have been leveraging the infrastructure of the United States, potentially indicating preparations for future attacks. | | | |

## Conclusion:

This month's threat activity underscores a dual challenge: adversaries are exploiting both legacy flaws and newly disclosed vulnerabilities across critical technologies. With vendors such as D-Link, Citrix, Microsoft, and N-able repeatedly surfacing in the KEV catalog, alongside relentless ransomware campaigns from Qilin, Akira, and Safepay targeting high-value sectors, the need for tighter alignment between patch management, threat intelligence, and incident readiness has never been more urgent. Loginsoft Vulnerability Intelligence (LOVI) addresses this need by delivering real-time, actionable insights that enable organizations to stay ahead of emerging threats, strengthen defenses, and protect critical assets. By shifting from a reactive to a proactive security posture, LOVI helps ensure resilience against an ever-evolving cyber threat landscape.

## External References:


- https://www.cisa.gov/news-events/alerts/2025/08/05/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/08/12/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/08/13/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/08/18/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/08/21/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/08/25/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/08/26/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/08/29/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2024/07/09/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2023/11/02/cisa-adds-one-known-exploited-vulnerability-catalog

- https://www.infosecurity-magazine.com/news/apt-threat-actors-exploit-ie-vulnerability/
- https://www.ic3.gov/CSA/2024/241216.pdf
- https://redcanary.com/blog/threat-intelligence/dripdropper-linux-malware/
- https://www.imperva.com/blog/imperva-detects-and-mitigates-rejetto-hfs-spray-and-pray-ransomware-trojan-campaign/
- https://www.bleepingcomputer.com/news/security/trend-micro-warns-of-endpoint-protection-zero-day-exploited-in-attacks/
- https://www.bleepingcomputer.com/news/apple/apple-emergency-updates-fix-new-actively-exploited-zero-day/
- https://www.bleepingcomputer.com/news/security/cisa-warns-of-n-able-n-central-flaws-exploited-in-zero-day-attacks/
- https://www.imperva.com/blog/imperva-detects-and-mitigates-rejetto-hfs-spray-and-pray-ransomware-trojan-campaign/