

Annual Report – 2024

Vulnerability Intelligence

Powered by
LOVI 

login:soft

Table of Contents

Executive Summary: Cybersecurity Landscape in 2024	6
Ransomware Activity in 2024.....	7
New Ransomware Observed in 2024.....	8
Elpaco	8
HellDown	8
Frag.....	8
Ymir.....	9
PSAUX	9
FOG.....	9
Zola	9
Brain Cipher.....	10
Estate.....	10
Ransomhub	10
Jasmin	11
BabLock / Rorschach	11
Inc Ransom	12
Bl00dy	12
NoEscape.....	12
Ransomware Insights – 2024	13
Vulnerabilities Abused by Botnet - 2024	17
Most Observed Vulnerabilities from our Sensors	19
Opensource Software Vulnerabilities abused by Threat Actors	20
CISA Industrial Control Systems (ICS) Medical CVE's abused by Malware	22
CISA Industrial Control Systems (ICS) General CVE's abused by Malware	25
Tracking CISA KEV in 2024.....	28
Comparison between 2024 and 2023.....	29
Monthly Breakdown of Trending/Actively Exploited Vulnerabilities	29
January	30
February	32
March	33
April	34
May	36
June.....	38
July.....	40
August	42

September.....	44
October.....	47
November.....	49
December	52
Sources Cited	54
Conclusion	57



Executive Summary: Cybersecurity Landscape in 2024

In 2024, the cybersecurity landscape witnessed a dramatic increase in vulnerabilities, with 144,987 new CVEs reported, a staggering 39.6% rise compared to 103,848 in 2023. This surge underscores the growing sophistication of cyber threats. Threat actors actively exploited over 100 CVEs, targeting various systems with more advanced tactics. Botnets, meanwhile, took advantage of over 20 vulnerabilities to launch widespread, large-scale attacks. Ransomware groups also proved their relentless adaptability, exploiting 30 CVEs to compromise networks and data. Alarming, 231 vulnerabilities were assigned the highest CVSS score of 10.0, emphasizing the critical urgency of addressing these risks.

The CISA Known Exploited Vulnerabilities (KEV) catalog expanded with 186 new additions, spotlighting the widespread targeting of prominent vendors. Microsoft led with 34 vulnerabilities, followed by Google and Apple with 13 and 7, respectively. These figures highlight the relentless focus on industry leaders by threat actors.

Beyond the tech giants, other key players were not spared. Ivanti added 11 vulnerabilities to the KEV catalog, while networking stalwarts D-Link and Cisco each saw 6 vulnerabilities exploited. VMware's 5 vulnerabilities and Fortinet's 4 demonstrated that virtualization and cybersecurity solutions remain attractive targets for attackers. Even Draytek, with 3 vulnerabilities, exemplified how adversaries left no stone unturned in their exploitation efforts.

The Ransomware landscape of 2024 was anything but static. RansomHub surged ahead, dethroning LockBit as the most prolific Ransomware operation of the year. Meanwhile, the cyber threat arena grew even more crowded with the arrival of Medusa, Akira, and Fog Ransomware, each bringing their own unique challenges to organizations worldwide.

Ransomware Activity in 2024

Ransomware activity in 2024 reached unprecedented levels, with Ransomhub overtaking LockBit as the most active group, recording over 200 confirmed victims. This year has also seen the emergence of 15 new Ransomware families, including [Mauri](#), [Elpaco](#), [HellDown](#), [Frag](#), [Ymir](#), [PSAUX](#), [FOG](#), [Zola](#), [Brain Cipher](#), [Estate](#), [Jasmin](#), [BabLock \(Rorschach\)](#), [Inc Ransom](#), [Bl00dy](#), and [NoEscape](#). Most of these groups have adopted double extortion tactics, exfiltrating sensitive data before encrypting systems, a strategy designed to amplify pressure on their victims and secure higher ransom payouts.

The Ransomware-as-a-service (RaaS) model has become increasingly popular among cybercriminals, with operators enlisting affiliates to distribute Ransomware in exchange for ransomware. This approach has greatly contributed to the rapid expansion and growing complexity of Ransomware attacks, making them more challenging to anticipate and defend against.

Ransomware attacks have increasingly targeted critical infrastructure sectors, such as healthcare, government organizations, energy and transportation, with potentially devastating consequences. Notable incidents include the LockBit attack in France, disrupting patient care and leading to the publication of sensitive data. The Wichita government also fell victim to a LockBit attack, causing significant disruption to city services. In the healthcare sector, a Catholic health system faced a BlackBasta attack, impacting clinical operations. The Ohio Lottery suffered a DragonForce attack, compromising player and employee data. These incidents highlight the evolving sophistication and devastating impact of Ransomware attacks, emphasizing the urgent need for robust cybersecurity defenses across all sectors.



New Ransomware Observed in 2024

Mauri

Mauri Ransomware represents a sophisticated and rapidly evolving threat that exploits the Apache ActiveMQ vulnerability, identified as CVE-2023-46604, to infiltrate systems and deploy malicious payloads. This vulnerability, a remote code execution flaw, allows attackers to compromise systems by exploiting weak authentication mechanisms in Apache ActiveMQ. After exploitation, Mauri Ransomware encrypts files using strong cryptographic algorithms such as AES-256 and RSA-4096 to secure encryption keys, making decryption without payment nearly impossible. In addition to file encryption, Mauri Ransomware has been observed deploying cryptocurrency miners as secondary payloads, further burdening compromised systems.

Vulnerabilities abused by Mauri Ransomware

1. [CVE-2023-46604](#) - Deserialization of untrusted data vulnerability in Apache ActiveMQ leads to remote code execution
 - <https://asec.ahnlab.com/en/85000/>

Elpaco

Elpaco Ransomware, a variant of the Mimic Ransomware family, poses a significant threat to organizations. It employs a multi-pronged approach to compromise systems, including exploiting vulnerabilities like Zerologon, brute-forcing RDP, and utilizing both legitimate and malicious tools. Once inside, Elpaco encrypts critical files, demands a ransom for decryption, and appends the ". ELPACO-team" extension to encrypted files.

Vulnerabilities abused by Elpaco Ransomware

1. [CVE-2020-1472](#) - Elevation of Privilege vulnerability in Microsoft Netlogon
 - <https://securelist.com/elpaco-ransomware-a-mimic-variant/114635/>

HellDown

HellDown Ransomware is an emerging cyber threat that targets Windows, Linux systems, and VMware infrastructures using a double-extortion strategy. This approach involves encrypting victims' data and threatening to leak it unless a ransom is paid. While Helldown shares code similarities with LockBit 3.0, it is distinct and remains under active development. Its evolution reflects the growing sophistication and adaptability of Ransomware attacks. The Ransomware primarily focuses on critical infrastructure and high-value organizations across industries such as manufacturing and healthcare, posing significant risks to essential services and sensitive data.

Vulnerabilities abused by HellDown Ransomware

1. [CVE-2024-42057](#) - OS Command Injection vulnerability in Zyxel firewalls
 - <https://blog.sekoia.io/helldown-ransomware-an-overview-of-this-emerging-threat/>

Frag

Frag Ransomware is a sophisticated and emerging cyber threat that exploits a critical vulnerability in Veeam Backup & Replication software (CVE-2024-40711) to gain initial access to target systems. This high-severity flaw allows remote code execution (RCE), enabling attackers to compromise backup servers, which are vital to an organization's disaster recovery infrastructure. After exploitation, Frag Ransomware conducts reconnaissance to identify valuable data repositories and employs robust encryption algorithms like AES-256 for data encryption and RSA for secure key exchange, effectively locking critical files. Leveraging double-extortion tactics, Ransomware not only encrypts data but also exfiltrates sensitive information, threatening to release it publicly unless a ransom is paid.

Vulnerabilities abused by Frag Ransomware

1. [CVE-2024-40711](#) - Remote Code Execution vulnerability in Veeam Backup & Replication

- <https://news.sophos.com/en-us/2024/11/08/veeam-exploit-seen-used-again-with-a-new-ransomware-frag/>

Ymir

Ymir Ransomware, discovered in late 2024, is a sophisticated and stealthy malware targeting Windows systems. It leverages Rusty Stealer for initial access, often through phishing emails or malicious links, and exploits vulnerabilities in widely used applications. Utilizing the qTox client, it enables encrypted communication between attackers and compromised systems. Ymir employs advanced anti-detection techniques, such as disabling endpoint protection, obfuscating payloads, and implementing delayed execution to evade forensic analysis. Operating through a modular framework, it allows attackers to deploy additional payloads or dynamically adapt their attack methods, making it a persistent and evolving threat to organizations across various sectors.

Vulnerabilities abused by Ymir Ransomware

1. [CVE-2024-40766](#) - Improper Access Control vulnerability in SonicWall SonicOS management access leads to crash

- <https://cionews.co.in/new-ymir-ransomware-targets-corporate-network/>

PSAUX

PSAUX Ransomware exploited vulnerabilities in CyberPanel, a popular web server control panel, impacting over 22,000 instances. By leveraging weaknesses like weak authentication and command injection flaws, attackers gained unauthorized access and deployed Ransomware, encrypting critical files.

Vulnerabilities abused by PSAUX Ransomware

1. [CVE-2024-51378](#) - OS Command Injection vulnerability in `getresetstatus` in `dns/views.py` and `ftp/views.py` in CyberPanel (aka Cyber Panel) through 2.3.6 and (unpatched) 2.3.7

- <https://censys.com/cve-2024-51378/>

FOG

FOG Ransomware, first identified in mid-2024, is an emerging cyber threat targeting educational institutions in the United States. Attackers exploit compromised VPN credentials to infiltrate networks, where they encrypt files on both Windows and Linux systems and delete backups to hinder recovery. Employing a double extortion strategy, FOG Ransomware exfiltrates sensitive data and threatens to leak it publicly unless a ransom is paid. The malware is characterized by its use of legitimate tools like PsExec and Advanced Port Scanner for lateral movement, as well as third-party services for data exfiltration.

Vulnerabilities abused by FOG Ransomware

1. [CVE-2024-40711](#) - Remote Code Execution vulnerability in Veeam Backup & Replication

- <https://findsec.org/index.php/blog/356-veeam-vulnerability-exploited-to-spread-ransomware>

2. [CVE-2024-40766](#) - Improper Access Control vulnerability in SonicWall SonicOS management access leads to crash

- <https://arcticwolf.com/resources/blog/arctic-wolf-labs-observes-increased-fog-and-akira-ransomware-activity-linked-to-sonicwall-ssl-vpn/>

Zola

Zola Ransomware, a variant of the Proton Ransomware family, is a C++-based malware that encrypts files, appends the ".zola" extension, and attempts to disable system recovery. It employs multi-threaded encryption for increased efficiency and targets both local and network files.

Vulnerabilities abused by Zola Ransomware

1. [CVE-2024-37085](#) - Authentication Bypass vulnerability in VMware ESXi
 - <https://socprime.com/blog/zola-ransomware-detection-proton-family-evolves-with-a-new-ransomware-variant-featuring-a-kill-switch/>

Brain Cipher

Brain Cipher Ransomware, emerging in June 2024, is a sophisticated threat linked to the LockBit Ransomware family. It employs a multi-pronged extortion strategy, combining file encryption with threats to leak stolen data via a TOR-based leak site. The Ransomware has been particularly active in Indonesia but has global implications, targeting critical sectors and businesses.

Vulnerabilities abused by Brain Cipher Ransomware

1. [CVE-2023-28252](#) - Privilege Escalation vulnerability in Microsoft Windows Common Log File System Driver
 - <https://otx.alienvault.com/pulse/6761a75807a4d64dc1d8a3d4>

Estate

Estate Ransomware is a sophisticated threat that targets organizations across various industries using advanced techniques. It exploits vulnerabilities in enterprise systems, especially in backup and disaster recovery solutions like Veeam Backup & Replication software. By leveraging critical vulnerabilities such as CVE-2024-40711, Ransomware gains unauthorized access to essential infrastructure components. Estate Ransomware typically infiltrates systems through phishing emails, malicious links, or compromised software updates, bypassing traditional security defenses by exploiting vulnerabilities in widely used enterprise tools. After exploitation inside the network, it conducts reconnaissance to locate and prioritize high-value assets.

Vulnerabilities abused by Estate Ransomware

1. [CVE-2023-27532](#) - Missing authentication vulnerability in Veeam Backup & Replication component
 - <https://www.group-ib.com/blog/estate-ransomware/>

Ransomhub

RansomHub is a fast-emerging and highly active Ransomware group that has become a significant cybersecurity threat since its debut in early 2024. Targeting a wide range of sectors, including manufacturing, retail, service providers, and healthcare, RansomHub employs a double-extortion strategy, encrypting victims' files and threatening to release stolen data publicly if the ransom is not paid. It typically gains initial access through phishing emails, malicious links, or exploiting enterprise system vulnerabilities. After exploitation, RansomHub uses tools like EDRKillShifter to disable endpoint detection and antivirus protections, along with advanced techniques such as obfuscation and privilege escalation through credential dumping and exploitation. The group conducts reconnaissance to identify high-value assets and spreads laterally across networks using remote services, PowerShell scripts, and custom payloads.

Vulnerabilities abused by Ransomhub Ransomware

1. [CVE-2023-48788](#) - SQL Injection vulnerability in Fortinet FortiClientEMS leads to code execution via specially crafted packets
 - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
2. [CVE-2023-46747](#) - Authentication Bypass vulnerability in F5 BIG-IP Configuration Utility leads to remote code execution
 - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>

3. [CVE-2023-46604](#) - Deserialization of untrusted data vulnerability in Apache ActiveMQ leads to remote code execution
 - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
4. [CVE-2023-3519](#) - Code Injection vulnerability in Citrix NetScaler ADC and NetScaler Gateway
 - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
5. [CVE-2023-27997](#) - Heap Based Buffer Overflow vulnerability in Fortinet FortiGate firewalls leads to arbitrary code or commands execution via specifically crafted requests
 - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
6. [CVE-2023-22515](#) - Broken Access Control Vulnerability in Atlassian Confluence Data Center and Server leads to privilege escalation
 - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
7. [CVE-2020-1472](#) - Elevation of Privilege vulnerability in Microsoft Netlogon
 - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
8. [CVE-2017-0144](#) - Remote Code Execution vulnerability in Windows SMB
 - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>

Jasmin

Jasmin is not typical Ransomware. It operates as a worm, rapidly spreading through networks and encrypting a wide range of files, including documents, photos, videos, and databases. This encryption renders the files inaccessible to users, effectively crippling operations. Unlike traditional Ransomware, Jasmin is primarily intended as a tool for red teams and ethical hackers to simulate realistic Ransomware attacks during security assessments.

Vulnerabilities abused by Jasmin Ransomware

1. [CVE-2024-27198](#) - Authentication Bypass Using an Alternate Path or Channel vulnerability in JetBrains TeamCity before 2023.11.4
 - <https://www.scworld.com/news/open-source-ransomware-rats-deployed-on-compromised-teamcity-servers>
2. [CVE-2024-27199](#) - Path Traversal vulnerability in JetBrains TeamCity before 2023.11.4
 - <https://www.scworld.com/news/open-source-ransomware-rats-deployed-on-compromised-teamcity-servers>

BabLock / Rorschach

BabLock/Rorschach Ransomware is a sophisticated threat with origins linked to the Babuk and LockBit Ransomware families. It employs advanced techniques, including DLL side-loading, to evade detection and rapidly encrypt critical files on compromised systems. This Ransomware targets various industries, including small and medium-sized enterprises, and demands a ransom for decryption.

Vulnerabilities abused by BabLock / Rorschach Ransomware

1. [CVE-2022-41352](#) - Arbitrary file upload vulnerability in Zimbra Collaboration (ZCS) 8.8.15 and 9.0 through amavis via a cpio loophole (extraction to /opt/zimbra/jetty/webapps/zimbra/public)
 - <https://www.sangfor.com/farsight-labs-threat-intelligence/cybersecurity/bablock-rorschach-ransomware>

Inc Ransom

INC Ransomware is a multi-extortion threat that targets enterprise networks by exploiting vulnerabilities and leveraging spear-phishing campaigns. This Ransomware is known for stealing sensitive data from victims and threatening to leak it online if the ransom demands are not met. The INC Ransomware group employs sophisticated tactics to compromise network devices, maintaining persistence and broadening its attack surface. Its operators exploit known vulnerabilities in unpatched systems to gain access, leveraging social engineering and phishing campaigns as initial entry points.

Vulnerabilities abused by Inc Ransom Ransomware

1. [CVE-2023-3519](#) - Code Injection vulnerability in Citrix NetScaler ADC and NetScaler Gateway
 - <https://www.sentinelone.com/anthology/inc-ransom/>
2. [CVE-2023-48788](#) - SQL Injection vulnerability in Fortinet FortiClientEMS leads to code execution via specially crafted packets
 - <https://www.reliaquest.com/blog/inc-ransom-attack-analysis/>
3. [CVE-2023-4966](#) - Buffer overflow vulnerability in NetScaler ADC and NetScaler Gateway leads to sensitive information disclosure
 - <https://www.secureworks.com/blog/gold-ionic-deploys-inc-ransomware>

Bl00dy

Bl00dy Ransomware has been actively targeting organizations, with a particular focus on the education sector. Exploiting vulnerabilities in PaperCut servers, specifically CVE-2023-27350, the attackers leverage exposed port 9191 to gain unauthorized access, bypassing user authentication and assuming administrative roles. Once inside the network, they exfiltrate sensitive data and encrypt systems, causing significant disruption. The attackers utilize 'cmd.exe' and 'powershell.exe' processes with elevated privileges to establish remote access, enabling lateral movement across compromised networks.

Vulnerabilities abused by Bl00dy Ransomware

1. [CVE-2023-27350](#) - Improper access control vulnerability in PaperCut NG and MF 22.0.5 (Build 63914) leads to Authentication bypass and arbitrary code execution.
 - https://www.csk.gov.in/alerts/Bl00dy_ransomware.html

NoEscape

NoEscape Ransomware, which emerged in May 2023, operates as a Ransomware-as-a-Service (RaaS) model, with its developers claiming to have created both the malware and its infrastructure from scratch, avoiding the use of code from other Ransomware families. The RaaS platform allows affiliates to design and deploy payloads targeting both Windows and Linux systems, expanding the malware's reach.

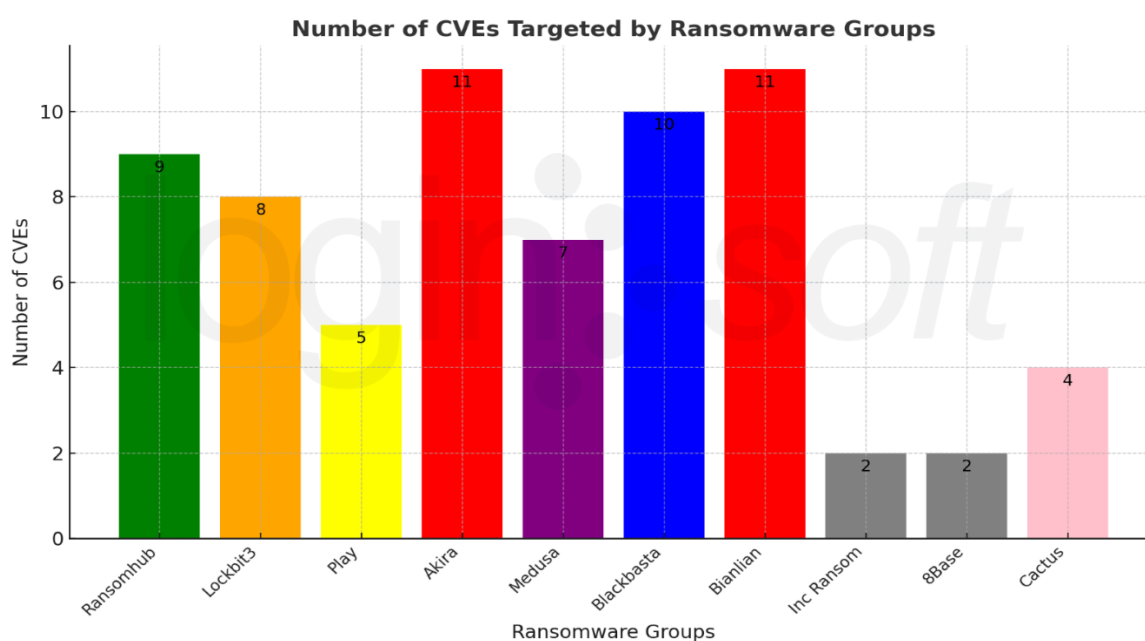
Vulnerabilities abused by NoEscape Ransomware

1. [CVE-2023-4966](#) - Buffer overflow vulnerability in NetScaler ADC and NetScaler Gateway leads to sensitive information disclosure
 - <https://unit42.paloaltonetworks.com/unit-42-ransomware-leak-site-data-analysis/>
2. [CVE-2019-12265](#) - Sensitive Information Disclosure vulnerability in Wind River VxWorks 6.5, 6.6, 6.7, 6.8, 6.9.3 and 6.9.4
 - <https://medium.com/@brotheralameen/malware-analysis-of-noescape-ransomware-56365f8d33ec>
3. [CVE-2019-12259](#) - NULL Pointer Dereference vulnerability in Wind River VxWorks 6.6, 6.7, 6.8, 6.9 and vx7 leads to denial of service
 - <https://medium.com/@brotheralameen/malware-analysis-of-noescape-ransomware-56365f8d33ec>

Ransomware Insights – 2024

Ransomware continues to be a critical and escalating threat to organizations, with incidents steadily rising over time. [Loginsoft's Vulnerability Intelligence](#) Report for 2024 delivers an in-depth analysis, exclusively focusing on vulnerabilities exploited by Ransomware groups throughout the year.

This report provides insights into vulnerabilities actively targeted across the internet, as observed through our globally deployed sensors. It also highlights the most affected sectors, offering a detailed perspective on industries that faced heightened risks from Ransomware attacks. These real-world observations offer a clear understanding of the vulnerabilities that threat actors are exploiting in the wild. Our Threat and Vulnerability Intelligence team, composed of seasoned researchers, meticulously analyzed thousands of vulnerabilities to uncover their root causes and assess the risks they pose to organizations. This report is designed to be a vital resource for organizations.



A bar graph illustrating Number of CVE's abused top 10 Ransomware – 2024

Source : [Loginsoft Vulnerability Intelligence - LOVI](#)

Ransomware	Description	No. of Affected Organizations 2024 (Jan – Dec)	Targeted Industries	Vulnerabilities Abused Most
Ransomhub	RansomHub, a rapidly emerging ransomware-as-a-service (RaaS) group, has quickly become a major threat in the cybercrime landscape. Operating on a double-extortion model, RansomHub encrypts victims' data and threatens to publicly release it unless a ransom is paid. This group has predominantly targeted critical infrastructure sectors. The sophistication of its campaigns is evident in its exploitation of vulnerabilities in widely used software, distribution of malware via phishing emails, and maintaining persistence on infected systems through techniques such as scheduled tasks.	611	Education	CVE-2023-3519
			Construction	CVE-2023-27997
			Government	CVE-2023-46604
			Bank	CVE-2023-22515
			Energy	CVE-2023-46747
				CVE-2023-48788
				CVE-2020-1472
				CVE-2020-0787
Lockbit3	LockBit 3.0, a potent Ransomware variant known as "LockBit Black," is a sophisticated cyber threat that emerged in 2022. Operating on a Ransomware-as-a-service (RaaS) model, it empowers affiliates to deploy the malware while sharing the profits with its developers. Renowned for its speed and efficiency, LockBit 3.0 leverages advanced encryption techniques and offers extensive customization options to attackers. Employing a double-extortion strategy, it exfiltrates sensitive data and threatens its public release if victims refuse to pay the ransom.	494	Manufacturing	CVE-2023-27350
			Technology	CVE-2023-27351
			Education	CVE-2023-40044
			Engineering	CVE-2023-4966
				CVE-2022-36537
				CVE-2022-41082
				CVE-2022-22279
				CVE-2019-7481
Play	Play Ransomware, also known as Playcrypt, is a highly sophisticated cyber threat that emerged in late 2022, primarily targeting large enterprises and critical infrastructure. It employs advanced techniques to maximize financial gain and operational impact, relying on double-extortion tactics that encrypt victim data while exfiltrating sensitive information. The attackers threaten to publish the stolen data if ransom demands are not met. Initial access is often achieved by exploiting vulnerabilities in public-facing applications or brute-forcing Remote Desktop Protocol (RDP) credentials. After exploitation, Play Ransomware leverages tools such as PowerShell scripts and exploits remote services to move laterally within a network. It strategically disables endpoint detection and antivirus solutions to avoid detection and ensure the success of its malicious payload.	366	Healthcare	CVE-2022-41080
			Media	CVE-2022-41082
			Technology	CVE-2022-41040
			Telecommunication	CVE-2020-12812
				CVE-2018-13379
Akira	Akira is a rapidly emerging Ransomware group, first identified in early 2023, and is operated by the threat actors known as GOLD SAHARA, PUNK SPIDER, and Storm-1567. Utilizing a Ransomware-as-a-service (RaaS) model, Akira employs a double extortion strategy by exfiltrating data before encrypting victims' devices. However, unlike some other Ransomware groups, Akira offers victims a degree of flexibility by allowing them to choose whether to pay for decryption assistance, data deletion, or both.	315	Bank	CVE-2024-40766
			Education	CVE-2024-40711
			Manufacture	CVE-2024-37085
			Finance	CVE-2023-27532
			Construction	CVE-2023-20269
				CVE-2023-20263
				CVE-2023-48788
				CVE-2022-40684
				CVE-2021-21972
				CVE-2020-3259
				CVE-2019-6693

Ransomware	Description	No. of Affected Organizations 2024 (Jan – Dec)	Targeted Industries	Vulnerabilities Abused Most
Hunters	Hunters International, identified as a Ransomware-as-a-Service (RaaS) provider, emerged after the detection of source code sharing resemblances with the infamous Hive Ransomware strain. Initial examination of the malware code revealed an estimated 60% similarity with samples from Hive Ransomware version 61. Detailed technical analysis proposes a plausible scenario in which the Ransomware could have been employed in activities associated with the recently dismantled Hive cartel.	235	Healthcare	UNKNOWN
			Education	
			Research	
			Education	
			Manufacturing	
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 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.	214	Healthcare	CVE-2024-37085
			Finance	CVE-2023-4966
			Technology	CVE-2023-48788
			Manufacturing	CVE-2022-2295
			Retail	CVE-2022-2294
				CVE-2022-21999
Qilin	The Qilin Ransomware has been in existence since August 2022, also recognized as Agenda, 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.	186	Education	UNKNOWN
			Healthcare	
			Automotive	
BlackBasta	Black Basta is a Ransomware group operating as Ransomware-as-a-service (RaaS) that was initially spotted in April 2022. It has since proven itself to be a formidable threat, as evidenced by its use of double-extortion tactics and expansion of its attack arsenal to include tools like the Qakbot trojan and PrintNightmare exploit.	171	Technology	CVE-2024-1708
			Insurance	CVE-2024-1709
			Manufacturing	CVE-2024-26169
			Utilities	CVE-2024-37085
			Real estate	CVE-2023-28252
			Finance	CVE-2021-42278
				CVE-2021-42287
				CVE-2021-34527
				CVE-2020-1472
Bianlian	BianLian is a Golang-based Ransomware. Initially operating as a Ransomware group focused on encrypting victims' data. BianLian has shifted its focus primarily to data extortion without encryption. The group exploits vulnerabilities in Remote Desktop Protocol (RDP) and other remote desktop services to gain initial access to networks, often leveraging stolen credentials. BianLian group adeptly utilizes open-source tools and command-line scripts to extract victims' data to a cloud storage controlled by attackers. Initially adopting a double-extortion model, the group shifted its strategy towards data exfiltration attacks after releasing a free decryptor.	169	Healthcare	CVE-2024-27198
			Banking	CVE-2023-27350
			Utilities	CVE-2022-37042
			Insurance	CVE-2022-27925
				CVE-2021-31207
				CVE-2021-34473
				CVE-2021-34523
				CVE-2021-4034
				CVE-2023-42793
				CVE-2022-37969
				CVE-2020-1472

Ransomware	Description	No. of Affected Organizations 2024 (Jan – Dec)	Targeted Industries	Vulnerabilities Abused Most
Inc Ransom	The Inc Ransom group is a sophisticated Ransomware operation targeting large-scale organizations and enterprises. Known for its diverse attack methods, the group employs a combination of vulnerability exploitation, spear-phishing campaigns, and tailored Ransomware deployment to compromise victims. Once inside a network, Inc Ransom uses advanced techniques to encrypt files, including partial encryption to optimize speed, targeting only key portions of large files.	165	Education	CVE-2023-3519
			Healthcare	CVE-2023-48788
			Government	
			Manufacturing	
			Information Technology	
Blacksuit	BlackSuit Ransomware, a sophisticated evolution of the Royal Ransomware strain, emerged as a prominent cyber threat in 2023. Known for its aggressive tactics, it employs a multi-extortion strategy, encrypting victims' data while exfiltrating sensitive information and threatening to leak it unless a ransom is paid. Initially linked to the Hermes Ransomware lineage, BlackSuit targets various sectors. The Ransomware is distributed by a group known as Ignoble Scorpis, which has ramped up attacks since March 2024, leveraging advanced evasion techniques to bypass defenses.	156	Information Technology	UNKNOWN
			Government	
			Retail	
			Manufacturing	
			Automotive	
8Base	Despite a significant surge in activity during the summer of 2023, the 8Base Ransomware group has largely operated in obscurity. Employing a combination of encryption and "name-and-shame" tactics, the group coerces victims into paying ransoms. Notably, 8Base follows an opportunistic compromise pattern, targeting victims across diverse industries. Despite the extensive compromises, details about the identities, methodology, and motivations behind the group's actions remain elusive. Examination of their Ransomware samples indicates the use of a customized Phobos with SmokeLoader.	148	Business service	CVE-2023-35078
			Finance	CVE-2023-3519
			Manufacture	
			Information Technology	
Meow	Meow Ransomware, a modified version of Conti-2 Ransomware, encrypts data on compromised servers using the ChaCha20 algorithm and demands ransom payment instructions via email or Telegram. The Ransomware's note is marked by the phrase "MEOW! MEOW! MEOW!" and logins repeating "meowcorp2022." Discovered in late 2022 as one of four strains derived from Conti's leaked code, Meow Ransomware operated from August 2022 to February 2023. In March 2023, a free decryptor was released, leading to a cessation of activity. However, the Meow group remains active in 2024, with nine victims reported so far, including three in March, targeting significant institutions.	130	Healthcare	UNKNOWN
			Finance	
			Education	
			Government	
			Manufacturing	
Cactus	Active since March 2023, Cactus Ransomware has primarily focused on U.S. manufacturing companies by exploiting vulnerabilities in VPN appliances to initiate unauthorized access. Notably, Ransomware exhibits unique evasion techniques, such as encrypting the malware binary to evade anti-malware detection.	99		CVE-2023-38035
			Food & Beverage	CVE-2023-41265
			Commercial entities	CVE-2023-41266
			Law Firms	CVE-2023-48365
			Manufacturing	

Vulnerabilities Abused by Botnet - 2024

Botnet activity in 2024 has been dominated by the resurgence of Mirai and its evolving variants, including Zerobot, EnemyBot, and MooBot. These botnets have leveraged their foundational Mirai codebase to exploit a wide range of vulnerabilities in IoT devices, routers, and servers. Zerobot and EnemyBot have aggressively expanded their attack surfaces, targeting Tenda Wi-Fi routers, and other internet-facing services, while MooBot has specialized in weaponizing flaws in IoT devices to propagate rapidly. This wave of botnet activity highlights the enduring threat posed by Mirai's adaptable framework, as attackers continue to refine their capabilities to launch larger and more sophisticated distributed denial-of-service (DDoS) attacks, steal data, and establish footholds within compromised networks. The persistence of these threats underscores the critical importance of patch management and proactive monitoring of vulnerable devices.

CVE-ID	Vendor	Product	Severity	Description	Botnet
CVE-2024-21887	Ivanti	Connect Secure and Policy Secure	Critical	A command injection vulnerability in the web components of Ivanti Connect Secure and Ivanti Policy Secure permits an authenticated administrator to execute arbitrary commands on the appliance by sending specially crafted requests.	Mirai
CVE-2024-3273	D-Link	NAS models	Critical	A Remote Code Execution (RCE) vulnerability that can be exploited to compromise internet-facing devices.	Mirai
CVE-2024-3721	TBK	DVR-4104 and DVR-4216	Medium	An OS command injection vulnerability in TBK DVR-4104 and DVR-4216	Mirai
CVE-2024-7029	AVTECH SECURITY Corporation	IP camera	High	Commands can be injected remotely and executed without requiring authentication.	Mirai
CVE-2024-36401	GeoSolutions	GeoServer	Critical	Code Injection vulnerability in GeoServer leads to remote code execution	JenX Condi
CVE-2024-4577	PHP Group	PHP	Critical	Argument Injection vulnerability in PHP CGI leads to remote code execution	Muhstik XMRig
CVE-2023-23333	SolarView	Compact	Critical	A command injection vulnerability in SolarView Compact allows attackers to bypass internal restrictions via the downloader.php endpoint, enabling the execution of arbitrary commands.	Mirai
CVE-2023-35885	CloudPanel	CloudPanel	Critical	Insecure file-manager cookie authentication vulnerability	Mirai
CVE-2023-46805	Ivanti	Connect Secure and Policy Secure	High	An authentication bypass vulnerability in the web component of Ivanti Connect Secure and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks.	Mirai
CVE-2023-26801	LB-LINK	LB-LINK Devicees	Critical	Command injection vulnerability in the LB-LINK	Mirai ZH1h9
CVE-2023-35885	CloudPanel	CloudPanel 2	Critical	Insecure file-manager cookie authentication vulnerability in CloudPanel 2	Mirai
CVE-2023-0669	Fortra	GoAnywhere MFT	High	Pre-authentication command injection vulnerability in Fortra GoAnywhere MFT due to deserializing an arbitrary attacker-controlled object	TrueBot
CVE-2023-22527	Atlassian	Confluence Data Center and Server	Critical	Template injection vulnerability in Out-of-Date Versions of Confluence Data Center and Server leads to remote code execution	Sysrv-botnet
					Enemybot Zerobot

CVE-ID	Vendor	Product	Severity	Description	Botnet
CVE-2022-1388	F5 Networks	BIG-IP	Critical	iControl REST authentication bypass vulnerability in F5 BIG-IP leads to RCE	Mirai
CVE-2022-30525	Zyxel	Firewall devices	Critical	An OS command injection vulnerability in the CGI program of Zyxel firewall devices could allow attackers to execute arbitrary commands on the system	Mirai
CVE-2022-26134	Atlassian	Confluence Server and Data Center	Critical	OGNL injection vulnerability in Confluence Server & Data Center	Mirai
CVE-2022-22963	VMware	Spring Cloud Function	Critical	A remote code execution vulnerability in Spring Cloud Function enables attackers to access and exploit local resources, potentially compromising the system.	Mirai
CVE-2022-22954	VMware	Workspace ONE Access and Identity Manager	Critical	Remote code execution vulnerability due to server-side template injection in VMware Workspace ONE Access and Identity Manager	Enemybot
					Mirai
CVE-2022-22947	VMware	Spring Cloud Gateway	Critical	Remote code execution vulnerability in Spring Cloud Gateway	Sysrv-botnet Enemybot Tsunami
CVE-2022-28956	D-Link	DIR	Critical	Improper Access Control vulnerabilty in getcfg.php component of D-Link DIR816L_FW206b01	MooBot
CVE-2022-30023	Tenda	ONT GPON	High	Command injection vulnerability via the Ping function in Tenda ONT GPON AC1200 Dual band WiFi HG9	Zerobot

Most Observed Vulnerabilities from our Sensors

Intel gathered through our [LOVI](#) platform, leveraging honeypot sensors strategically deployed across diverse demographic locations, has provided valuable insights into emerging threats. These sensors have captured extensive activity linked to various CVEs, offering a unique perspective on how vulnerabilities are being exploited in real-world scenarios. This approach not only highlights geographic variations in attack patterns but also underscores the importance of distributed monitoring systems for identifying and mitigating risks effectively.

CVE-ID	Vendor	Product	Severity	Description
CVE-2023-26801	LB-LINK	LB-LINK Devices	Critical	Command injection vulnerability in LB-LINK BL-AC1900_2.0 1.0.1, BL-WR9000 2.4.9, BL-X26 1.2.5 and BL-LTE300 1.0.8
CVE-2022-30023	Tenda	ONT GPON	High	Command injection vulnerability via the Ping function in Tenda ONT GPON AC1200 Dual band WiFi HG9 v1.0.1
CVE-2022-25168	Apache	Hadoop	Critical	Command injection vulnerability in org.apache.hadoop.fs.FileUtil.unTarUsingTar in Apache Hadoop 2.0.0 to 2.10.1, 3.0.0. Alpha to 3.2.3, 3.3.0 to 3.3.2
CVE-2021-38647	Open Management	Open Management Infrastructure	Critical	Improper Initialization vulnerability in Open Management Infrastructure
CVE-2021-22205	GitLab	Gitlab-Exiftool	Critical	Remote code execution vulnerability in Gitlab-Exiftool
CVE-2020-29662	Harbor	Harbor 2.0	Medium	Sensitive Information disclosure vulnerability in Harbor 2.0
CVE-2018-0296	Cisco	Cisco Adaptive Security Appliance Firepower Threat Defense	High	Denial-of-Service and Directory Traversal vulnerability in Cisco Adaptive Security Firepower Threat Defense due to improper input validation
CVE-2017-6316	Citrix	NetScaler SD-WAN devices	Critical	Arbitrary shell command execution vulnerability in Citrix NetScaler SD-WAN devices via a CGISESSID cookie
CVE-2017-17215	Huawei	Huawei HG532	High	Remote code execution vulnerability in Huawei HG532
CVE-2017-16894	Laravel	Laravel Framework	High	Sensitive information disclosure vulnerability in Laravel framework
CVE-2015-2051	D-Link	DIR-645 Wired/Wireless Router	Critical	Arbitrary command execution vulnerability in D-Link DIR-645 Wired/Wireless Router
CVE-2014-9390	Git	Git	Critical	Command Execution Vulnerability in Git
CVE-2013-5936	Open-Xchange	Hazelcast cluster API	Medium	Sensitive information disclosure vulnerability in The Hazelcast cluster API in Open-Xchange AppSuite
CVE-2007-1860	Apache	Tomcat JK Web Server Connector	Medium	Path traversal vulnerability in Apache Tomcat JK Web Server Connector 1.2.x before 1.2.23 via a crafted prefix JkMount

Opensource Software Vulnerabilities abused by Threat Actors

OSS Intelligence involves gathering and analyzing information about vulnerabilities across all available open-source 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
CVE-2024-9680	Mozilla	Firefox	Critical	Use After Free vulnerability in Animation timelines in Firefox	RomCom
CVE-2024-7971	Google	Chrome	Critical	Type Confusion vulnerability in V8 in Google Chrome	FudModule
CVE-2024-4947	Google	Chrome	Critical	Type Confusion vulnerability in V8 in Google Chrome	Manuscript
CVE-2024-43047	Qualcomm	Digital Signal Processor (DSP) Service	High	Use After Free vulnerability in Qualcomm in Digital Signal Processor (DSP) Service	NoviSpy
CVE-2024-38402	Qualcomm	Digital Signal Processor (DSP) Service	High	Use After Free vulnerability in Qualcomm DSP Service	NoviSpy
CVE-2024-36401	GeoServer	GeoServer	Critical	Code Injection vulnerability in GeoServer leads to remote code execution	Mozi
					AndroXgh0st
					EagleDoor
					Condi.
					JenX.
CVE-2024-33060	Qualcomm	Digital Signal Processor (DSP) Service	High	Use After Free vulnerability in Qualcomm DSP Service	NoviSpy
CVE-2024-23897	Jenkins	Jenkins	Critical	Arbitrary File Read vulnerability in Jenkins leads to remote code execution	RansomEXX
CVE-2024-23334	Aiohttp	Aiohttp	High	Path Traversal vulnerability in aiohttp leads to unauthorized access to arbitrary files	ShadowSyndicate
CVE-2024-21455	Qualcomm	Digital Signal Processor (DSP) Service	High	Untrusted Pointer Dereference vulnerability in Qualcomm DSP Service	NoviSpy
CVE-2023-50386	Apache	Solr	High	Unrestricted Upload of File with Dangerous Type in Apache Solr	Mirai
CVE-2023-46604	Apache	ActiveMQ	Critical	Deserialization of untrusted data vulnerability in Apache ActiveMQ leads to remote code execution	CoinMiner
					Andariel
					z0Miner
					Ransomhub
					KrustyLoader
					Hezb
					Godzilla Webshell
					Kinsing
					SparkRAT
					HELLOKITTY
					Mauri

CVE-ID	Vendor	Product	Severity	Description	Abused by Malware
CVE-2023-3824	PHP	PHP	Critical	Improper restriction of operations within the bounds of a memory buffer vulnerability in PHP leads to remote code execution	LockBit
CVE-2018-7602	Drupal	Drupal	Critical	A remote code execution vulnerability in multiple subsystems of Drupal	STOP Ransomware



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

CISA's Industrial Control Systems (ICS) Medical security capabilities are specifically designed to safeguard the functionality and security of medical industrial control systems. These systems encompass the essential hardware and software that support healthcare operations, along with the tools used by medical professionals to manage them effectively. By focusing on the integrity and resilience of ICS Medical environments, CISA aims to reduce risks and enhance the security of critical healthcare infrastructure.

CVE-ID	Vendor	Product	Severity	Description	Abused by Malware
CVE-2020-1938	Apache	Tomcat	Critical	Remote code execution vulnerability in Apache Tomcat	Bifrost
CVE-2019-0708	Microsoft	Remote Desktop Services	Critical	Remote code execution vulnerability in Microsoft Remote Desktop Services	InvisiMole
					BlackHunt
					Amelia
					Vohuk
					NYX Ransomware
					Redeemer
					MedusaLocker
					WatchBog
					LEMONDUCK
CVE-2018-10115	7-Zip	7-Zip	High	Remote Code Execution vulnerability in 7-Zip	Houdini
CVE-2017-8464	Microsoft	Windows	High	LNK Remote Code Execution Vulnerability	Bad Rabbit
CVE-2017-7269	Microsoft	Windows	Critical	Buffer overflow vulnerability in the WebDAV service in (IIS) in Microsoft Windows Server 2003 R2 leads to arbitrary code execution	NotPetya
CVE-2017-0213	Microsoft	Windows COM	High	Elevation of Privilege Vulnerability in Windows COM	STOP Ransomware
					Lucifer
					LEMONDUCK
					XMRig
					BlackSquid
					Hydraq
					XMRig
					PLEAD
					Phobos
CVE-2017-0148	Microsoft	SMBv1 Server	High	Improper input validation vulnerability in Microsoft SMBv1 Server leads to remote code execution	Ragnarok
					ASPXSpy
					Clambling
					PlugX
					Netwalker
					Bitlocker
					Dharma
					RagnarLocker
					Nefilim
					Satan
					WannaCryptor
					Lucifer

CVE-ID	Vendor	Product	Severity	Description	Abused by Malware
CVE-2017-0199	Microsoft	Office/WordPad	High	Remote Code Execution Vulnerability in Microsoft Office/WordPad	AndeLoader
					Ramsay
					Petya
					Azorult
					njRAT
					Agent Tesla
					SmokeLoader
					Grooboor
					BISKVIT
					Helminth
CVE-2017-0148	Microsoft	SMBv1 Server	High	Improper input validation vulnerability in Microsoft SMBv1 Server leads to remote code execution	Remcos
					Satan
CVE-2017-0147	Microsoft	Windows SMB	High	Sensitive information disclosure from process memory in Windows SMB via a crafted packet	WannaCryptor
					Lucifer
					Satan
					WannaMiner
					CoinMiner
					ROKRAT
CVE-2017-0146	Microsoft	Windows SMB	High	Remote code execution vulnerability in Microsoft Windows SMB	NotPetya
					WannaCry
					TrickBot
					Satan
					Lucifer
CVE-2017-0145	Microsoft	Windows SMB	High	Remote Code Execution Vulnerability in Windows SMB	Emotet
					TrickBot
					WannaCryptor
CVE-2017-0144	Microsoft	Windows SMB	High	Remote Code Execution vulnerability in Windows SMB	Petya
					Lucifer
					EternalRocks
					WannaCry
					Ransomhub
					Satan
					Uiwix
					Petya
					PurpleFox EK
					DirtyMoe
CVE-2017-0143	Microsoft	Windows SMB	High	Remote code execution vulnerability in Windows SMB	STOPRansomware
					LEMONDUCK
					NotPetya
					TrickBot
					DoublePulsar
					XMRig
					Bad Rabbit
					Lucifer
CVE-2017-0143	Microsoft	Windows SMB	High	Remote code execution vulnerability in Windows SMB	WannaCry
					Satan
					Petya
					NotPetya
					Ryuk
CVE-2017-0143	Microsoft	Windows SMB	High	Remote code execution vulnerability in Windows SMB	DoublePulsar
					DoublePulsar

CVE-ID	Vendor	Product	Severity	Description	Abused by Malware
CVE-2017-0101	Microsoft	Windows Transaction Manager	High	Elevation of privilege vulnerability in Windows Transaction Manager	Conti
CVE-2017-0022	Microsoft	XML Core Services	Medium	Information Disclosure vulnerability in Microsoft XML Core Services	Astrum EK
CVE-2017-0005	Microsoft	Windows GDI	High	Windows GDI Elevation of Privilege Vulnerability	Neutrino EK
CVE-2014-9222	AllegroSoft	RomPager	High	Authentication security bypass vulnerability in AllegroSoft RomPager leads to memory corruption	Zirconium
CVE-2008-4250	Microsoft	Windows	High	Server Service Vulnerability in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta	Mirai
					Conficker
					Stuxnet

login:soft

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

CISA's Industrial Control Systems (ICS) security capabilities are designed to protect the functionality and security of industrial control systems across diverse sectors. These systems include the essential hardware and software that support operational processes, as well as the tools that operators rely on to manage them efficiently. By prioritizing the integrity and resilience of ICS environments, CISA works to mitigate risks and strengthen the security of critical infrastructure nationwide.

CVE-ID	Vendor	Product	Severity	Description	Malware Abused
CVE-2024-1709	ConnectWise	ScreenConnect	Critical	Authentication Bypass Using an Alternate Path or Channel vulnerability in ConnectWise ScreenConnect leads to sensitive information disclosure	LockBit Black Basta BI00dy TODDLERSHARK Androxxgh0st KrustyLoader ZIPLINE WARPWIRE LIGHTWIRE CHAINLINE FRAMESTING BUSHWALK XMRig Mirai RedTail MASOL RAT GHOSTSPIDER SNAPPYBEE Hemigate
CVE-2024-21887	Ivanti	Connect Secure and Policy Secure Gateways	Critical	Command Injection vulnerability in Ivanti Connect Secure and Ivanti Policy Secure Gateways	
CVE-2024-23334	aiohttp	aiohttp	High	Path Traversal vulnerability in aiohttp leads to unauthorized access to arbitrary files	ShadowSyndicate
CVE-2024-23897	Jenkins	Jenkins	Critical	Arbitrary File Read vulnerability in Jenkins leads to remote code execution	RansomEXX
CVE-2024-3273	D-Link	NAS devices	Critical	Command Injection Vulnerability in D-Link NAS devices	Mirai
CVE-2024-36401	GeoServer	GeoServer	Critical	Code Injection vulnerability in GeoServer leads to remote code execution	SideWalk CoinMiner JenX Condi EagleDoor Androxxgh0st Mozi
CVE-2024-3721	TBK	DVR Devices	Medium	OS Command Injection vulnerability in TBK DVR-4104 and DVR-4216 up to 20240412	Mirai
CVE-2024-4577	PHP	PHP CGI	Critical	Argument Injection vulnerability in PHP CGI leads to remote code execution	Tellyouthepass Muhstik XMRig Ghost RAT RedTail Msupedge Androxxgh0st Mozi

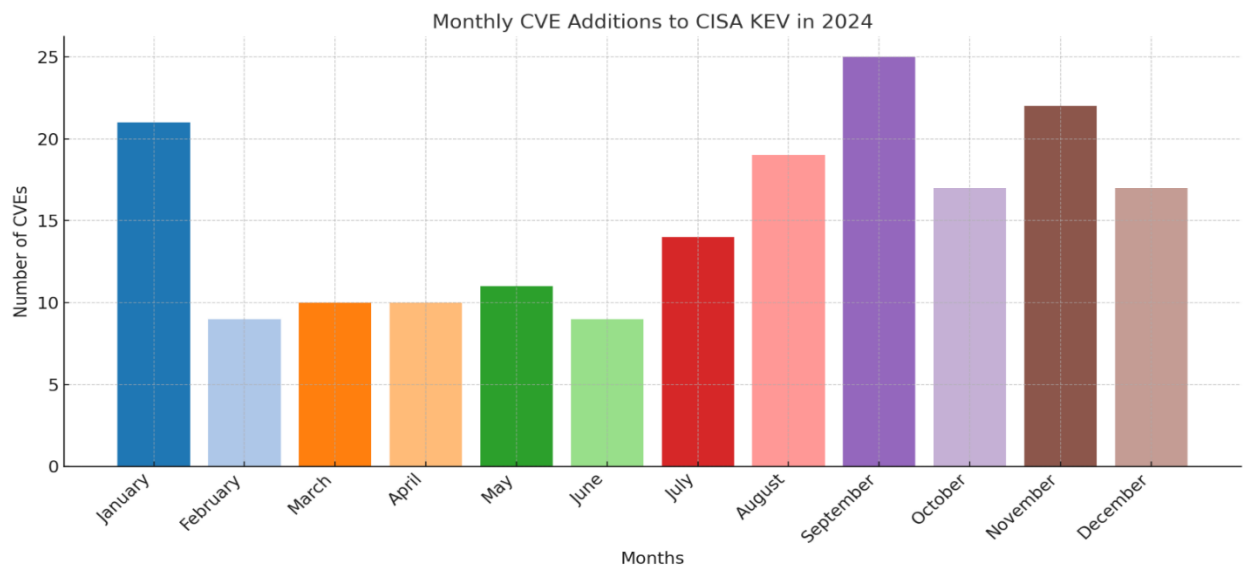
CVE-ID	Vendor	Product	Severity	Description	Malware Abused
CVE-2024-7029	AVTECH	IP Camera	Critical	Command Injection vulnerability in AVTECH SECURITY Corporation IP camera AVM1203 firmware through FullImg-1023-1007-1011-1009	Mirai
CVE-2023-0669	Fortra	GoAnywhere	High	Pre-authentication command injection vulnerability in Fortra GoAnywhere MFT due to deserializing an arbitrary attacker-controlled object	Clon TrueBot LockBit BlackCat
CVE-2023-20198	Cisco	IOS XE Software	Critical	Privilege escalation vulnerability in web UI feature of Cisco IOS XE Software	BadCandy
CVE-2023-22527	Confluence	Data Center and Server	Critical	Template injection vulnerability in Out-of-Date Versions of Confluence Data Center and Server leads to remote code execution	Cerber Sysrv-botnet XMRig Godzilla Webshell
CVE-2023-23333	SolarView	Compact	Critical	Command injection vulnerability in SolarView Compact	Mirai
CVE-2023-26801	LB-Link	LB-Link Devices	Critical	Command injection vulnerability in LB-LINK BL-AC1900_2.0 1.0.1, BL-WR9000 2.4.9, BL-X26 1.2.5 and BL-LTE300 1.0.8	Mirai IZ1H9
CVE-2023-35885	CloudPanel	CloudPanel	Critical	Insecure file-manager cookie authentication vulnerability in CloudPanel 2	Mirai
CVE-2023-38646	Metabase	Metabase	Critical	Remote code execution vulnerability in Metabase open source and Metabase Enterprise	Kinsing DreamBus Monero Miner XMRig
CVE-2023-42793	JetBrains	TeamCity	Critical	Authentication bypass using an alternate path or channel vulnerability in JetBrains TeamCity leads to remote code execution	BianLian FeedLoad RollSling HazyLoad ForestTiger GraphicalProton CoinMiner KrustyLoader
CVE-2023-46747	F5 Networks	BIG-IP	Critical	Authentication Bypass vulnerability in F5 BIG-IP Configuration Utility leads to remote code execution	Ransomhub

CVE-ID	Vendor	Product	Severity	Description	Malware Abused
CVE-2023-46805	Ivanti	Connect Secure and Policy Secure Gateways	High	Authentication Bypass vulnerability in Ivanti Connect Secure and Ivanti Policy Secure Gateways	SPAWNSLOTH
					SPAWNANT
					KrustyLoader
					ZIPLIN
					XMRig
					TERRIBLETEA
					TONERJAM
					SPAWNSNAIL
					SPAWNMOLE
					Mirai
					RedTail
					GHOSTSPIDER
					SNAPPYBEE
					MASOL RAT
					Crowdoor
CVE-2023-4966	NetScaler	ADC and Gateway	High	Buffer overflow vulnerability in NetScaler ADC and NetScaler Gateway leads to sensitive information disclosure	SparrowDoor
					Hemigate
					Zingdoor
					LockBit
					Medusa
					BlackCat
					NoEscape
					Play
					Inc Ransom

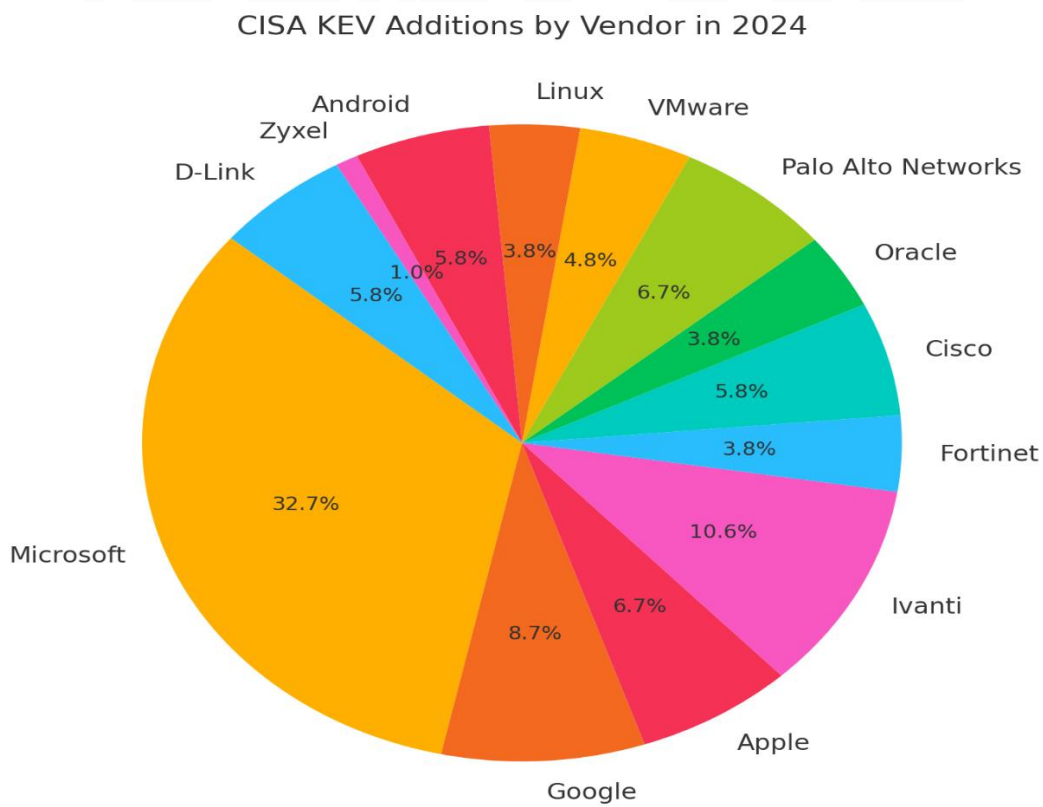


Tracking CISA KEV in 2024

The year 2024 witnessed a dynamic pattern of additions to the CISA Known Exploited Vulnerabilities (KEV) catalog, peaking in September with 25 entries, followed by November’s 22 and August’s 19. While the early months, like January 21, laid a strong foundation, mid-year months such as June and July added 9 and 14 respectively, keeping the momentum steady. These fluctuations remind us that cyber adversaries are never dormant, urging organizations to bolster their defenses year-round.



A bar graph illustrating the monthly distribution of CISA KEV additions throughout 2024

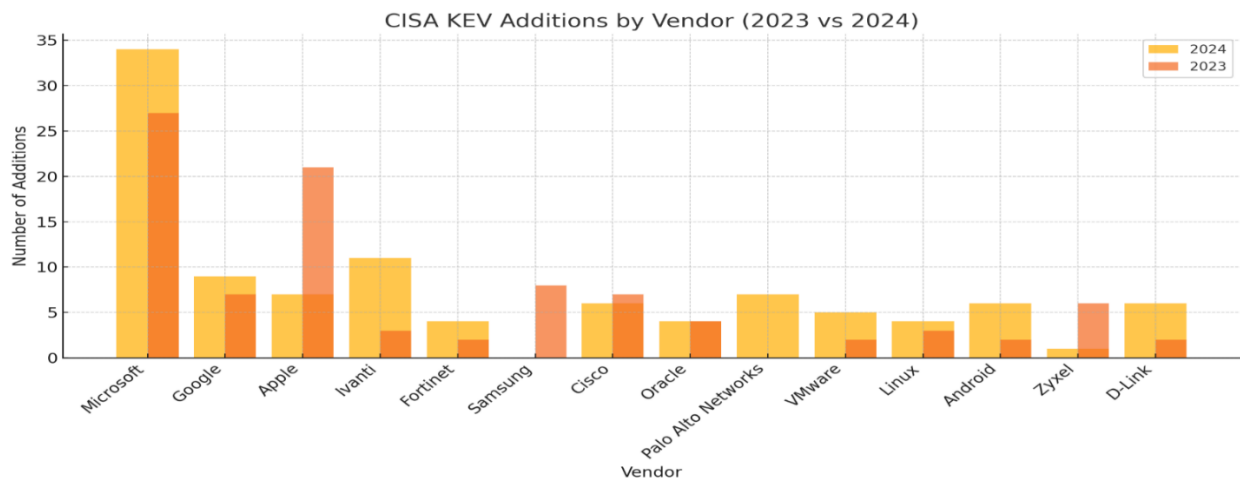


A pie chart showcasing the distribution of CISA KEV additions by vendor for 2024

Comparison between 2024 and 2023

In 2024, Microsoft led the pack with a sharp rise in CISA KEV additions, jumping from 27 in 2023 to 34; a testament to its critical role in vulnerability disclosures. In contrast, Apple saw a dramatic decline, with entries plummeting from 21 to just 7, raising questions about evolving threat landscapes. Google and Cisco reported modest upticks, climbing to 9 and 6 additions respectively, hinting at steady activity in addressing vulnerabilities. Meanwhile, Samsung stood out for its absence, with no new entries in 2024 compared to 8 the previous year, signaling either improved security or shifting focus in threat detection.

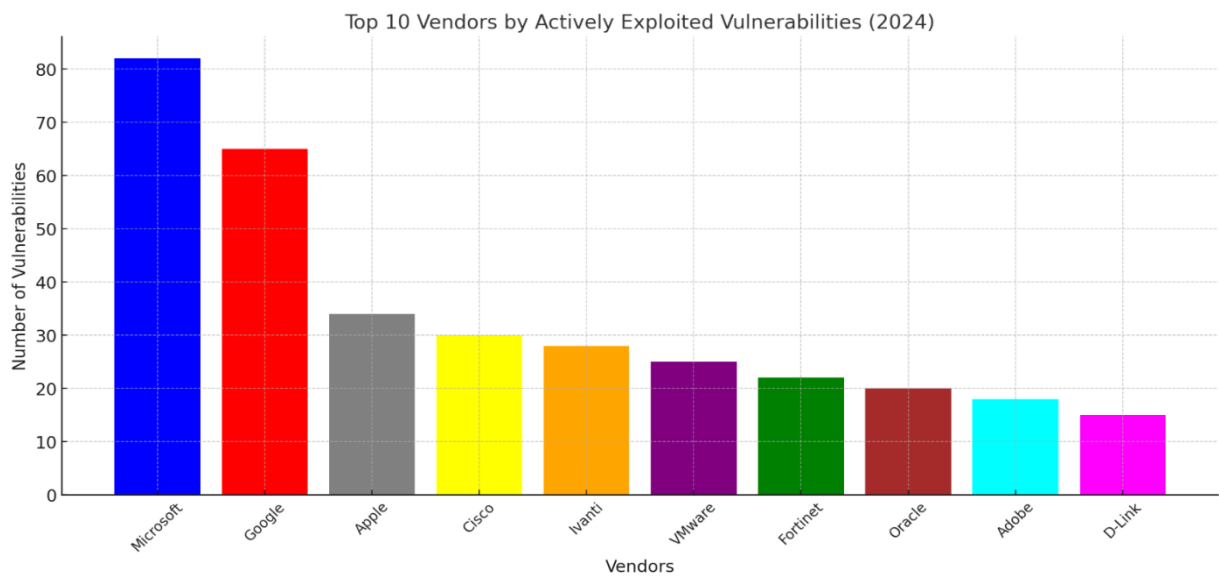
The CISA KEV catalog in 2024 featured vulnerabilities from 58 distinct vendors, down from 65 in 2023, reflecting a change in the variety of affected organizations.



Comparative Bar Graph of CISA KEV Additions by Vendor: 2024 vs. 2023

Monthly Breakdown of Trending/Actively Exploited Vulnerabilities

In 2024, the cybersecurity landscape was marked by several vulnerabilities that garnered 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.



A bar graph depicting the top 10 actively exploited vendors and their corresponding vulnerability count

Source: [Loginsoft Vulnerability Intelligence - LOVI](#)

January

In January 2024, 21 vulnerabilities were added to the CISA Known Exploited Vulnerabilities (KEV) catalog. Among these, five vulnerabilities were actively exploited as zero days, underscoring the urgency of immediate remediation efforts. The vulnerabilities spanned various categories, including four involving remote code execution (RCE), three related to code injection, and three tied to the deserialization of untrusted data.

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2024-21887	Ivanti	Connect Secure, Policy Secure	A command injection vulnerability in Ivanti Connect Secure and Ivanti Policy Secure enables an authenticated administrative user to execute arbitrary commands on the vulnerable systems by sending specially crafted requests.	Yes	Yes	FALSE
CVE-2024-21893	Ivanti	Connect Secure, Policy Secure, and Neurons Server	A critical server-side request forgery vulnerability in the Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA that allows an unauthorized attacker to access restricted resources on the vulnerable server.	Yes	Yes	FALSE
CVE-2024-0519	Google	Chromium V8	An out-of-bound memory access vulnerability in the Google Chrome V8 JavaScript and WebAssembly engine that can be leveraged by threat actors to perform remote code execution attack on the vulnerable system.	No	Yes	TRUE
CVE-2024-23222	Apple	Multiple products	A type of confusion vulnerability in the Apple WebKit that allows attackers to execute arbitrary commands on the vulnerable systems with the help of crafted web information.	No	Yes	TRUE
CVE-2023-7101	Comprehensive Perl Archive Network (CPAN)	Spreadsheet:ParseExcel	An arbitrary code execution vulnerability presents in the perl module used for parsing Excel files which arises as a result of using a string-type "eval" function with unvalidated input from a file.	Yes	Yes	TRUE
CVE-2023-38203	Adobe	ColdFusion	Deserialization of Untrusted Data vulnerability present in Adobe ColdFusion that can potentially result in Arbitrary code execution. This vulnerability can be exploited without any user interaction.	No	Yes	FALSE
CVE-2023-29300	Adobe	ColdFusion	Deserialization of Untrusted Data vulnerability present in Adobe ColdFusion that can potentially result in Arbitrary code execution. This vulnerability can be exploited without any user interaction.	No	Yes	FALSE
CVE-2023-27524	Apache	Superset	An authentication bypass and remote code execution vulnerability that is caused due to an insecure default configuration which might result in enabling the attackers to administrator access on target server.	No	Yes	TRUE
CVE-2023-41990	Apple	Multiple products	A vulnerability in the ADJUST TrueType font instruction that permits remote code execution through a malicious and invisible iMessage.	No	Yes	FALSE
CVE-2023-23752	Joomla	Joomla	An unauthorized access vulnerability which allows unauthorized users to access confidential information on the website.	No	Yes	FALSE

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2023-29357	Microsoft	SharePoint server	A critical elevation of privilege vulnerability in the Microsoft SharePoint Server. Due to this vulnerability, SharePoint would skip the signature validation which can enable the attacker to impersonate any authenticated user on the system.	No	Yes	FALSE
CVE-2023-6548	Citrix	NetScaler ADC and NetScaler Gateway	A critical remote code execution vulnerability in the Citrix NetScaler ADC and NetScaler Gateway appliances that can be leveraged by an unauthenticated attacker with least privileges to execute arbitrary code on vulnerable systems.	No	Yes	FALSE
CVE-2023-6549	Citrix	NetScaler ADC and NetScaler Gateway	A denial of service (DoS) vulnerability in the Citrix NetScaler ADC and NetScaler Gateway that enables unauthenticated attackers to disrupt the operations of vulnerable systems.	No	Yes	FALSE
CVE-2023-35082	Ivanti	Endpoint Manager Mobile (EPMM) and MobileIron Core	An authentication bypass vulnerability in Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core which enables unauthenticated remote attackers to potentially access the functionalities and resources that are restricted.	No	Yes	FALSE
CVE-2023-34048	VMware	vCenter Server	An out-of-bounds write vulnerability in DCERPC protocol affecting VMware vCenter Server that can allow malicious threat actors with network access to execute arbitrary commands on the system.	Yes	Yes	FALSE
CVE-2023-22527	Atlassian	Confluence Data Center and Server	A remote code execution vulnerability in the Atlassian Confluence Server and Data Center that allows an attacker to exploit and get complete control over the vulnerable servers without requiring any login credentials.	No	Yes	FALSE
CVE-2022-48618	Apple	Multiple products	An improper authentication vulnerability in multiple Apple products that can be leveraged by an attacker with arbitrary read and write capabilities to bypass security mechanism in Apple operating systems.	No	Yes	FALSE
CVE-2018-15133	Laravel	Framework	A critical remote code execution vulnerability in Laravel PHP web framework, that could enable remote attackers to execute arbitrary commands on the vulnerable systems.	Yes	Yes	TRUE
CVE-2016-20017	D-Link	DSL-2750B	A command injection vulnerability in the D-Link DSL-2750B devices that allows remote, unauthenticated command injection via the login. CGI cli parameter.	Yes	Yes	TRUE

February

In February, nine vulnerabilities were added to the CISA Known Exploited Vulnerabilities (KEV) catalog, impacting multiple vendors, four from Microsoft, one vulnerability each from Google, Fortinet and Cisco.

Notably, three vulnerabilities were actively exploited as zero-days. Among the attack types, two involved elevation of privilege (EoP) and two were related to security feature bypass.

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2024-1709	ConnectWise	ScreenConnect	An authentication bypass vulnerability using an alternate path or channel could enable attackers to directly access sensitive information on critical systems.	Yes	Yes	FALSE
CVE-2024-21410	Microsoft	Windows	Elevation of Privilege vulnerability in the Microsoft Exchange Server	No	Yes	FALSE
CVE-2024-21412	Microsoft	Windows	Security feature bypass vulnerability in the Internet Shortcut files.	Yes	Yes	FALSE
CVE-2024-21351	Microsoft	Windows	A security feature bypass vulnerability in the Windows SmartScreen	No	Yes	FALSE
CVE-2024-21762	Fortinet	FortiOS	Out-of-bounds- write vulnerability in the Fortinet FortiOS that allows attackers to execute unauthorized code or commands via specially crafted requests.	Yes	Yes	FALSE
CVE-2023-29360	Microsoft	Windows	An elevation of privilege vulnerability in the Microsoft streaming service	Yes	Yes	FALSE
CVE-2023-43770	Roundcube	Webmail	A persistent Cross-site scripting (XSS) vulnerability in the Roundcube Webmail	Yes	Yes	TRUE
CVE-2023-4762	Google	Chrome	Type confusion vulnerability in the V8 JavaScript engine that allows an unauthenticated remote attacker to execute arbitrary commands via a specially crafted HTML page.	Yes	Yes	TRUE
CVE-2020-3259	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	An information disclosure vulnerability that could allow unauthenticated remote attackers to collect memory contents on the affected devices.	Yes	Yes	FALSE

March

In March, 10 vulnerabilities were added to the CISA KEV catalog, including two from Microsoft and two from Apple. Notably, three vulnerabilities were actively exploited as zero-days. Among the attack types, two involved memory corruption and three were code injection vulnerabilities.

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2024-21338	Microsoft	Windows Kernel	Elevation privilege vulnerability in the Windows Kernel	Yes	Yes	FALSE
CVE-2024-27198	JetBrains	TeamCity	An authentication bypass vulnerability that allows attackers to perform administrative actions on the vulnerable systems.	Yes	Yes	FALSE
CVE-2024-23225	Apple	IOS and iPadOS	Memory Corruption vulnerability in Apple iOS, iPadOS leads to kernel memory protections bypass	No	Yes	FALSE
CVE-2024-23296	Apple	IOS and iPadOS	A memory corruption vulnerability in RTKit, Apple's proprietary real-time operating system, which could allow attackers to circumvent kernel memory protections.	No	Yes	FALSE
CVE-2023-24955	Microsoft	Windows SharePointServer	A remote code execution vulnerability in the Microsoft SharePoint Server	No	Yes	FALSE
CVE-2023-48788	Fortinet	FortiClientEMS	An SQL injection vulnerability in the Fortinet FortiClientEMS that allows attackers to execute unauthorized code via specially crafted packets	Yes	Yes	FALSE
CVE-2023-21237	Google	Android	This vulnerability allows the attacker to hide foreground service notification leading to information disclosure without any additional privileges.	No	Yes	TRUE
CVE-2021-44529	Ivanti	CSA	A code injection vulnerability in Ivanti CSSA enables unauthenticated users to execute arbitrary code with restricted permissions.	Yes	Yes	FALSE
CVE-2021-36380	Sunhillo	SureLine	An unauthenticated OS command injection vulnerability	Yes	Yes	FALSE
CVE-2019-7256	Linear	eMerge E3-Series	A command injection vulnerability in the Linear eMerge E3-Series devices	Yes	Yes	FALSE

April

In April, 10 vulnerabilities were added to the CISA KEV catalog, including two from Microsoft, two from Cisco, two from D-Link, and two from the Android Framework. Notably, seven vulnerabilities were actively exploited as zero-days. Among the attack types, eleven involved Remote Code Execution (RCE), two were elevation of privilege (EOP) vulnerabilities, one was a security feature bypass, and one was a denial-of-service (DoS) vulnerability.

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2024-29988	Microsoft	Windows	Security feature bypass vulnerability in the SmartScreen prompt	Yes	Yes	FALSE
CVE-2024-4040	Crush FTP	Crush FTP	An improper input validation vulnerability in the Crush FTP which allows an attacker to exploit the vulnerable Crush FTP server to escape the Virtual File system (VFS) sandbox.	No	Yes	FALSE
CVE-2024-20359	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	A vulnerability in the Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software that enabled the preloading of VPN clients and plug-ins that can be leveraged by a local attacker to run arbitrary code with root-level access.	Yes	Yes	FALSE
CVE-2024-29988	Microsoft	Windows	Security feature bypass vulnerability in the SmartScreen prompt	Yes	Yes	FALSE
CVE-2024-4040	Crush FTP	Crush FTP	An improper input validation vulnerability in the Crush FTP which allows an attacker to exploit the vulnerable Crush FTP server to escape the Virtual File system (VFS) sandbox.	No	Yes	FALSE
CVE-2024-20359	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	A vulnerability in the Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software that enabled the preloading of VPN clients and plug-ins that can be leveraged by a local attacker to run arbitrary code with root-level access.	Yes	Yes	FALSE
CVE-2024-20353	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software that could enable an unauthorized remote attacker to force the device to unexpectedly reload, resulting in a denial of service (DoS) situation.	Yes	Yes	FALSE
CVE-2024-3400	Palo Alto Networks	PAN-OS	A command injection vulnerability affecting PAN-OS's GlobalProtect Gateway functionality. This vulnerability can be leveraged by a remote, unauthenticated attacker to execute arbitrary codes on an exploited firewall with root privileges.	Yes	Yes	TRUE
CVE-2024-3273	D-Link	NAS devices	A Remote Code Execution (RCE) vulnerability that can be exploited to compromise internet-facing devices.	Yes	Yes	FALSE

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2024-3272	D-Link	NAS devices	A backdoor vulnerability that can allow attackers to utilize hardcoded credentials to access the web management interface without any authorization	Yes	Yes	FALSE
CVE-2024-29748	Google	Android	A vulnerability in the Pixel firmware that allows for elevation of privilege.	No	Yes	TRUE
CVE-2024-29745	Google	Android	A bootloader component vulnerability in Google Pixel that could lead to information exposure.	No	Yes	TRUE
CVE-2022-38028	Microsoft	Windows Print spooler	An elevation of privilege vulnerability in the Windows Print spooler that can be leveraged by an attacker to gain system privileges.	Yes	Yes	FALSE



May

In May 2024, a total of 24 vulnerabilities were actively exploited, with 12 of these added to the CISA KEV catalog. Notably, seven zero-day flaws were in play, including four in Google Chrome and two in Microsoft products. Among the actively exploited vulnerabilities, critical issues included five instances of Remote Code Execution (RCE) and two use-after-free vulnerabilities, underscoring the growing sophistication of cyber threats.

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2024-4671	Google	Chrome	A use after free in visuals vulnerability in Google Chrome which when successfully exploited can permit an attacker to install programs, view, change or delete data and create new user accounts with administrative privileges.	No	Yes	TRUE
CVE-2024-4947	Google	Chrome	A type of confusion bug in the V8 JavaScript engine that could allow an attacker to perform remote code execution attacks	No	Yes	TRUE
CVE-2024-4761	Google	Chrome	An out-of-bounds write issue in Google Chrome's V8 JavaScript Engine which can be leveraged by the attacker to execute arbitrary code and crash the application.	No	Yes	TRUE
CVE-2024-5274	Google	Chrome	A type of confusion vulnerability in Google Chrome's V8 JavaScript and WebAssembly engine that can result in unexpected crashes and even remote code execution.	No	Yes	TRUE
CVE-2024-30051	Microsoft	Windows DWM core library	An Elevation of Privilege (EoP) vulnerability in the DWM core Library in Microsoft Windows that can be exploited by a local attacker to gain SYSTEM privileges.	Yes	Yes	FALSE
CVE-2024-30040	Microsoft	Windows DWM core library	A security feature bypass vulnerability in the MSHTML (Trident) Engine in Microsoft Windows that could be exploited by the attacker by using social engineering tactics via email, social media to convince a target user to open a specially crafted malicious document and then execute an arbitrary code.	No	Yes	FALSE
CVE-2024-4978	JAVS	Viewer	A software supply chain attack in JAVS Viewer, a component of the JAVA Suite 8 that allows users to produce, manage, publish, and view digital recordings of legal proceedings, business meetings	Yes	No	FALSE
CVE-2023-43208	NextGen Healthcare	Mirth Connect	A pre-authenticated remote code execution vulnerability in NextGen Mirth Connect that was exploited successfully against several health organizations by NodeZero, a pentesting tool of Horizon3.ai.	No	Yes	FALSE
CVE-2023-7028	GitLab	Community Edition and Enterprise edition	An account-take-over vulnerability that could allow an attacker to take over the GitLab administrator account without requiring user interaction.	No	Yes	FALSE
CVE-2023-20198	Cisco	IOS XE software	A privilege escalation vulnerability in the Web UI feature, that could allow an attacker to create an administrative user.	Yes	Yes	FALSE
CVE-2023-40000	LiteSpeed Technologies	LiteSpeed Cache plugin	A stored cross-site scripting (XSS) vulnerability in the LiteSpeed Cache plugin for WordPress that allows an unauthorized user to elevate privileges by using specially crafted HTTP requests.	Yes	No	FALSE
CVE-2023-26801	LB-LINK	Wireless router models	A command injection vulnerability in LB-LINK products which when successfully exploited could allow a remote attacker to execute arbitrary commands on the affected systems.	Yes	No	FALSE
CVE-2021-40655	D-Link	DIR-605 router	An information disclosure vulnerability in the D-Link- DIR-605 B2 Firmware Version: 2.01 MT that can be leveraged by the attacker to retrieve login credentials by forging a post request to the /getcfg.php page.	No	Yes	FALSE

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2020-17519	Apache	Flink	A directory traversal vulnerability in the REST API of Apache Flink that enables an attacker to potentially read any file on the local filesystem of the JobManager.	No	Yes	FALSE
CVE-2015-2051	D-Link	DIR-645 routers	A remote code execution vulnerability that permits the attackers to execute malicious commands via a GetDeviceSettings action on the HNAP interface of targeted devices remotely.	Yes	Yes	FALSE
CVE-2014-100005	D-Link	DIR600 Router	A Cross-Site Request Forgery (CSRF) vulnerability present in the D-Link DIR600 Router that allows the attacker to perform malicious actions on behalf of an authenticated user which results in creation of fraud administrator accounts and exposure of sensitive user credentials	No	Yes	FALSE
CVE-2008-0166	Debian Project	OpenSSL library	A vulnerability in the OpenSSL library used by Debian-based operating systems, including Debain and Ubuntu. This vulnerability arises due to a predictable random number generator which makes it easier for the remote attackers to carry out brute force attacks against cryptographic keys.	No	No	TRUE

login:soft

June

June 2024 saw 19 vulnerabilities being actively exploited, with 9 of these vulnerabilities being listed in the CISA KEV catalog. The affected products included key platforms such as Microsoft, Oracle, Android, Progress, PHP Group, and Linux. Six of the exploited vulnerabilities were zero-day flaws, while seven were associated with Remote Code Execution (RCE).

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2024- 4610	Arm Ltd	Bifrost GPU Kernel Driver & Valhall GPU Kernel Driver	A vulnerability in Mali GPU kernel Driver that involves improper GPU memory processing operations that can be leveraged by a local non-privileged user to gain access to already free memory.	No	Yes	FALSE
CVE-2024-4577	PHP Group	PHP	A critical argument injection vulnerability in PHP that can be leveraged to achieve remote code execution.	Yes	Yes	FALSE
CVE-2024-30080	Microsoft	Message	A critical remote code execution vulnerability in Microsoft Message Queuing (MSMQ) that can be exploited by a remote attacker to execute malicious commands and gain complete control over the affected system.	No	No	FALSE
		Queuing (MSMQ)				
CVE-2024-32896	Google	Pixel Firmware	A critical elevation of privilege vulnerability in the Pixel Firmware.	No	Yes	TRUE
CVE-2024-4358	Progress	Telerik Report Server	Critical authentication bypass vulnerability in the Progress Telerik Report Server which when exploited successfully can enable an attacker to take complete control over the affected server.	No	Yes	FALSE
CVE-2024-26169	Microsoft	Windows Error Reporting service	An elevation of privilege vulnerability in the Windows Error Reporting service that can be exploited to gain SYSTEM privileges.	Yes	Yes	FALSE
CVE-2024-6045	D-Link	Wireless routers	An undisclosed factory testing backdoor that could enable attackers within the local network to gain unauthorized access to the router's Telnet service by utilizing default administrator credentials.	No	No	FALSE
CVE-2024-37902	DeepJavaLibrary (DJL)	DeepJavaLibrary (DJL)	A critical path traversal vulnerability in the Deep Java Library (DJL) which enables the attackers to rewrite important system files and take complete control of the affected systems	No	No	TRUE
CVE-2024-28995	SolarWinds	Serv-U file transfer software	A directory traversal vulnerability in SolarWinds Serv-U file transfer software that enables unauthorized attackers to potentially read confidential files present in the server hosting the software.	No	No	FALSE
CVE-2024-29973	Zyxel	NAS326 and NAS542 devices	A command injection vulnerability in the "setCookie" parameter that enables an unauthenticated attacker to execute OS commands via specially crafted HTTP POST request.	Yes	No	FALSE
CVE-2024-5806	Progress	MOVEit file transfer software product	A critical authentication bypass vulnerability affecting the SSH File Transfer Protocol (SFTP) module in the Progress MOVEit file transfer software product.	No	No	FALSE
CVE-2023-32191	Rancher Labs	Kubernetes Engine	A critical vulnerability in the Rancher Kubernetes Engine poses a severe risk to the security and integrity of Kubernetes clusters.	No	No	TRUE
CVE-2023-21839	Oracle	WebLogic Server	A remote code execution vulnerability in the Oracle WebLogic Server which could potentially result in the attackers taking full control of the affected system.	Yes	Yes	FALSE

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2023-20867	VMware	VMware Tools	An authentication bypass vulnerability in VMware tools that allows a fully compromised ESXi host to fail to authenticate host-to-guest operations thereby impacting on the confidentiality and integrity of the guest virtual machine.	Yes	Yes	TRUE
CVE-2022-22948	VMware	VCenter Server	An information disclosure vulnerability in the VMware vCenter that exposes sensitive information due to improper file permissions.	Yes	No	FALSE
CVE-2022-41328	Fortinet	FortiOS	An improper path traversal vulnerability in the Fortinet FortiOS that can allow privileged attackers to read and write arbitrary files via crafted CLI commands.	Yes	Yes	FALSE
CVE-2022-42475	Fortinet	FortiProxy	A critical heap-based buffer overflow vulnerability in the SSL VPN component of Fortinet's FortiOS and FortiProxy devices which when successfully exploited by a remote unauthenticated attacker can lead to arbitrary code execution on the affected devices.	Yes	Yes	FALSE
CVE-2022-24816	GeoSolutions	JAI-EXT	A critical remote code execution vulnerability in the JAI-EXT which is an open-source project that aims to extend the Java Advanced Imaging (JAI) API which can be leveraged by an attacker via a malicious Jiffle script provided through a network request.	No	Yes	TRUE
CVE-2022-2586	The Linux Foundation	Linux Kernel	A use-after-free vulnerability in the nftables (NFT) framework of the Linux Kernel which when successfully exploited can allow an attacker to execute arbitrary codes with root privileges.	Yes	Yes	TRUE
CVE-2020-13965	Roundcube	Webmail	A storage Cross-site scripting (XSS) vulnerability in the Roundcube Webmail that leverages an attacker to bypass the script filter and execute malicious JavaScript on the affected systems	No	Yes	TRUE
CVE-2020-1472	Microsoft	Windows Server	This vulnerability also known as "ZeroLogon", is a critical security vulnerability that affects Windows Server operating systems and was disclosed by Microsoft in August 2020. It resides in the Netlogon Remote Protocol (MS-NRPC), which is used for authentication in Active Directory environments. Specifically, the vulnerability arises in the Netlogon authentication process.	Yes	Yes	TRUE
CVE-2019-9082	ThinkPHP	ThinkPHP	A critical remote code execution vulnerability in the Open Source BMS which exists due to improper handling of the user input in the invokefunction function of the ThinkPHP framework. This can be exploited by the attacker via specially crafted HTTP request including a malicious code in it.	Yes	Yes	FALSE
CVE-2018-20062	ThinkPHP	ThinkPHP	A critical remote code execution vulnerability in NoneCms which exists due to improper verification on user-supplied input within the filter parameter of the ThinkPHP framework. This can be exploited by the attacker by crafting a malicious URL that injects a code when the program processes it.	Yes	Yes	FALSE

July

In July 2024, 17 vulnerabilities were actively exploited, with 14 new additions to the CISA KEV catalog. Among these, Microsoft accounted for three, followed by VMware and ServiceNow with 2 vulnerabilities each. Additionally, four of the vulnerabilities were zero-day exploits, while Remote Code Execution (RCE) was observed in four cases.

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2024-20399	Cisco	NX-OS Software	A vulnerability in Cisco NX-OS allows an authenticated user with administrative privileges to execute arbitrary commands with root-level access by manipulating input within specific CLI commands.	Yes	Yes	FALSE
CVE-2024-23692	Rejetto	HTTP File Server (HFS)	A critical flaw in Rejetto HTTP File Server enables remote attackers to execute malicious commands on the system by submitting specially crafted HTTP requests.	Yes	Yes	FALSE
CVE-2024-39891	Twilio	Authy API	Twilio's Authy API contained a vulnerability that allowed anyone to check if a phone number was registered for Authy without authentication.	Yes	Yes	FALSE
CVE-2024-6387	OpenSSH	OpenSSH	A flaw in OpenSSH allows attackers to gain unrestricted root access to vulnerable Linux systems without requiring any authentication. This vulnerability arises from a timing-based attack that exploits race conditions in the OpenSSH server.	Yes	No	TRUE
CVE-2024-38080	Microsoft	Windows Hyper-V	A vulnerability in Microsoft Windows Hyper-V allows attackers to bypass user restrictions and gain unrestricted system-level access.	No	Yes	FALSE
CVE-2024-38112	Microsoft	MSHTML Platform	A vulnerability in Windows MSHTML allows attackers to disguise malicious content as legitimate content by embedding it within a specially crafted HTML file.	Yes	Yes	FALSE
CVE-2024-29510	Artifex	Ghostscript	A vulnerability in Artifex Ghostscript allows attackers to bypass security restrictions by injecting malicious code through format string manipulation.	No	No	TRUE
CVE-2024-5441	Webnus	Modern Events Calendar plugin	The Modern Events Calendar plugin allows attackers to upload harmful files to a WordPress website, potentially leading to a site takeover.	No	No	FALSE
CVE-2024-28995	OSGeo	GeoServer and GeoTools	A flaw in SolarWinds Serv-U allows unauthorized users to access and view sensitive files on the server.	Yes	Yes	FALSE
CVE-2024-34102	SolarWinds	Serv-U	A critical vulnerability in Adobe Commerce and Magento allows attackers to execute malicious code by exploiting improper handling of XML data, potentially leading to a complete system takeover.	No	Yes	TRUE
CVE-2024-4879	Adobe	Commerce	A critical flaw in ServiceNow's UI Macros allows anyone to execute malicious code within the platform without requiring any login.	No	Yes	FALSE
CVE-2024-37085	ServiceNow	Now Platform	A flaw in VMware ESXi's Active Directory integration allowed attackers to bypass authentication and gain complete control of the system.	Yes	Yes	FALSE
CVE-2023-28252	VMware	ESXi hypervisors	A flaw in Windows allows users with limited privileges to escalate their access to the highest level of system control.	Yes	Yes	FALSE
CVE-2023-45249	Microsoft	Common Log File System Driver	Acronis Cyber Infrastructure (ACI) contained a critical flaw that allowed attackers to bypass security measures and gain complete control of the system by exploiting default passwords.	No	Yes	FALSE

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2022-22948	Acronis	Cyber Infrastructure	A security flaw in VMware vCenter allows unauthorized access to sensitive information due to improper file protection.	Yes	Yes	FALSE
CVE-2012-4792	VMware	vCenter Server	A Use-after-free vulnerability in the Microsoft Internet Explorer which, when successfully exploited, allows an attacker to execute malicious commands on the affected systems.	Yes	Yes	FALSE



August

In August 2024, a total of 27 vulnerabilities were actively exploited, with 19 of them added to the CISA KEV catalog. These included eight Microsoft vulnerabilities, two each from Google, Apache, and Dahua. Among the exploited vulnerabilities, six involved Remote Code Execution (RCE), while three were related to authentication bypass, and another three were use-after-free vulnerabilities.

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2024-7971	Google	Chrome	A type of confusion bug in the V8 JavaScript and WebAssembly engine that can enable a remote attacker to exploit heap corruption via a crafted HTML page.	Yes	Yes	TRUE
CVE-2024-7965	Google	Chrome	An inappropriate implementation bug in the V8 JavaScript and Web Assembly engine that could enable a remote attacker to potentially exploit heap corruption via a crafted HTML page.	No	Yes	FALSE
CVE-2024-28000	LiteSpeed Technologies	Cache WordPress plugin	An unauthenticated privilege escalation vulnerability in the LiteSpeed Cache WordPress plugin that allows unauthenticated attackers to escalate their privileges and gain administrative access on the affected sites	No	No	FALSE
CVE-2024-36971	The Linux Foundation	Linux Kernel	A use after free vulnerability in the Linux kernel network routing component. Requiring elevated privileges, this flaw can be exploited to manipulate network traffic behavior.	Yes	Yes	TRUE
CVE-2024-39717	Versa Networks	Director GUI	A file upload vulnerability impacting the "Change Favicon" feature that allows threat actor to upload malicious files disguised as harmless PNG images.	Yes	Yes	FALSE
CVE-2024-7029	Avtech	Security cameras	A command injection vulnerability in the Avtech Security cameras that could be leveraged by the attacker to inject commands over the network and execute them without any authentication requirement.	Yes	No	FALSE
CVE-2024-38856	Apache	OFBiz	An incorrect authorization vulnerability in the Apache OFBiz, that can be exploited by remote and unauthenticated attackers to execute arbitrary code on vulnerable systems.	No	Yes	FALSE
CVE-2024-32113	Apache	OFBiz	A path traversal vulnerability in the Apache OFBiz that can potentially lead to remote code execution.	Yes	Yes	FALSE
CVE-2024-4885	Progress	WhatsUp Gold	A remote code execution vulnerability in the Progress WhatsUp Gold that can allow attackers to execute arbitrary code remotely without requiring any authentication.	Yes	No	FALSE
CVE-2024-28986	SolarWinds	Web Help Desk	Deserialization of Untrusted Data vulnerability in SolarWinds Web Help Desk through 12.8.3 leads to remote code execution.	No	Yes	FALSE
CVE-2024-38107	VMware	ESXi hypervisor	Use After Free vulnerability in Windows Power Dependency Coordinator leads to privilege escalation	No	Yes	FALSE
CVE-2024-38193	Microsoft	Windows Power Dependency Coordinator	Use After Free vulnerability in Windows Ancillary Function Driver for WinSock leads to privilege escalation	No	Yes	FALSE
CVE-2024-38106	Microsoft	Windows Ancillary Function Driver	Privilege Escalation vulnerability in Microsoft Windows Kernel	No	Yes	FALSE
CVE-2024-38189	Microsoft	Windows Kernel	Remote Code Execution vulnerability in Microsoft Project	No	Yes	FALSE
CVE-2024-38178	Microsoft	Project	Memory Corruption vulnerability in Windows Scripting Engine leads to remote code execution	No	Yes	FALSE
CVE-2024-38213	Microsoft	Windows Scripting Engine	Security Feature Bypass vulnerability in Microsoft Windows SmartScreen.	No	Yes	FALSE

CVE-ID	Vendor	Product	Description	Abused by Malware	CISA KEV	OSS
CVE-2024-23897	Microsoft	Windows SmartScreen	A path traversal vulnerability in the Jenkins Command Line Interface (CLI) that could potentially lead to code execution.	Yes	Yes	TRUE
CVE-2024-7262	Jenkins	Command Line Interface (CLI)	An improper path validation vulnerability in the Kingsoft WPS Office, that could allow attackers to execute arbitrary code on a user's system.	Yes	No	FALSE
CVE-2023-22527	WPS	Office	A template injection vulnerability found in the older versions of Confluence Data Center and Server that enables unauthenticated attacker to achieve remote code execution on the vulnerable systems.	Yes	Yes	FALSE
CVE-2022-0185	Atlassian	Confluence Data Center and Confluence Server	A heap-based buffer overflow vulnerability in the Filesystem Context functionality of Linux Kernel that enables an attacker to gain elevated privileges on the affected systems.	Yes	Yes	TRUE
CVE-2021-33044	The Linux Foundation	Linux Kernel	Authentication bypass vulnerability in the Dahua IP cameras that can be exploited remotely during login process by sending specially crafted data packets to the target system.	No	Yes	FALSE
CVE-2021-33045	Dahua	IP camera	Authentication bypass vulnerability in the Dahua IP cameras that can be exploited remotely during login process by sending specially crafted data packets to the target system.	No	Yes	FALSE
CVE-2021-31196	Dahua	IP camera	A remote code execution vulnerability in the Microsoft Exchange Server that can be leveraged by an attacker to execute arbitrary codes on the affected server.	No	Yes	FALSE
CVE-2018-0824	Microsoft	Windows Exchange Server	A deserialization of untrusted data vulnerability in Microsoft COM for Windows which can lead to remote code execution.	Yes	Yes	FALSE
CVE-2017-0199	Microsoft	Windows	A remote code execution vulnerability in Microsoft Office and WordPad that can be leveraged by an attacker to take complete control of the affected system.	Yes	Yes	FALSE
CVE-2017-11882	Microsoft	Office and WordPad	A memory corruption vulnerability in Microsoft Office allows attackers to execute malicious code by exploiting the software's improper handling of in-memory data.	Yes	Yes	FALSE

September

A total of 35 vulnerabilities were actively exploited this month, with 25 being added to the CISA KEV catalog. These include five Microsoft vulnerabilities, four in Adobe Flash Player, three each in Ivanti and DrayTek, and two in Oracle products. Notably, five zero-day vulnerabilities, all in Microsoft products were actively exploited. Among the attack types, 10 involved Remote Code Execution (RCE), while others included privilege escalation, SQL injection, security feature bypass, authentication bypass, and local file inclusion.

CVE-ID	Vendor	Product	Description	Abused by malware	CISA KEV	OSS
CVE-2024-43461	Microsoft	Windows MSHTML platform	A spoofing vulnerability in the Windows MSHTML platform.	Yes	Yes	FALSE
CVE-2024-38014	Microsoft	Windows Installer	An elevation of privilege vulnerability in the Windows Installer.	No	Yes	FALSE
CVE-2024-38217	Microsoft	Windows Mark of the Web	A security feature bypass vulnerability in the Windows Mark-of-the-Web (MotW).	No	Yes	FALSE
CVE-2024-38226	Microsoft	Publisher	A security feature bypass vulnerability in the Microsoft Publisher.	No	Yes	FALSE
CVE-2024-43491	Microsoft	Windows	A remote code execution vulnerability in the Microsoft Windows Update.	No	No	FALSE
CVE-2024-6670	Progress	WhatsUp Gold	A SQL injection vulnerability in WhatsUp Gold allows attackers to bypass authentication and gain unauthorized access to encrypted user passwords.	No	Yes	FALSE
CVE-2024-8190	Ivanti	Cloud Services Appliance (CSA)	An OS command injection vulnerability in Ivanti Cloud Service Appliance that enables a remote authenticated attacker to achieve remote code execution.	No	Yes	FALSE
CVE-2024-8963	Ivanti	Cloud Services Appliance (CSA)	A path traversal vulnerability in Ivanti Cloud Service Appliance that can enable an attacker to bypass admin authentication and execute arbitrary commands on the appliance.	No	Yes	FALSE
CVE-2024-7593	Ivanti	Virtual Traffic Manager (vTM)	Critical authentication bypass vulnerability in Ivanti's Virtual Traffic Manager (vTM) that enables remote unauthenticated attackers to bypass authentication of the admin panel.	No	Yes	FALSE
CVE-2024-36401	OSGeo	GeoServer GeoTools	An eval injection vulnerability in GeoServer that could result in remote code execution.	Yes	Yes	TRUE
CVE-2024-45506	HAProxy Technologies	HAProxy	A vulnerability in HAProxy can create an endless loop under certain conditions, leading to a system crash and a remote denial-of-service (DoS) attack.	No	No	FALSE
CVE-2024-40766	SonicWall	SonicWall Firewall	An improper access control vulnerability in the SonicWall SonicOS management access and SSLVPN which could allow unauthorized access to resources and, under certain conditions, result in a firewall crash.	Yes	Yes	FALSE
CVE-2024-7120	Raisecom Technology Co., Ltd.	Raisecom MSG1200, MSG2100E, MSG2200, MSG2300	A command injection vulnerability in the RAISECOM Gateway devices enables remote attackers to execute malicious commands on the vulnerable systems.	No	No	FALSE

CVE-ID	Vendor	Product	Description	Abused by malware	CISA KEV	OSS
CVE-2024-47076	OpenPrinting	Common UNIX Printing System	The function cfGetPrinterAttributes5 does not properly validate or sanitize the IPP attributes received from an IPP server, allowing attacker-controlled data to be passed through the rest of the CUPS system.	No	No	TRUE
CVE-2024-47175	OpenPrinting	Common UNIX Printing System	The ppdCreatePPDFromIPP2 function fails to validate or sanitize IPP attributes when writing them to a temporary PPD file, enabling the injection of attacker-controlled data into the resulting PPD file.	No	No	TRUE
CVE-2024-47176	OpenPrinting	Common UNIX Printing System	Listens on UDP INADDR_ANY:631 , accepting packets from any source, which can trigger a Get-Printer-Attributes IPP request directed to a URL controlled by an attacker.	No	No	FALSE
CVE-2024-47177	OpenPrinting	Common UNIX Printing System	The foomatic-rip utility allows arbitrary command execution through the FoomaticRIPCommandLine PPD parameter, potentially enabling exploitation by attackers.	No	No	FALSE
CVE-2023-48788	Fortinet	FortiClient EMS	A SQL injection vulnerability in Fortinet's FortiClient EMS Software enables attackers to execute malicious code on vulnerable systems and gain initial access.	Yes	Yes	FALSE
CVE-2023-38831	RARLAB	WinRAR	A vulnerability in WinRAR allows attackers to execute malicious code on a system by tricking users into opening a specially crafted archive file.	Yes	No	FALSE
CVE-2023-25280	D-Link	DIR-820 Router	An OS command injection vulnerability in the D-Link routers that can enable an attacker to elevate privileges to root via a crafted payload.	Yes	Yes	FALSE
CVE-2022-21445	Oracle	JDeveloper	A remote code execution vulnerability in the Oracle JDeveloper application that enables attackers to execute arbitrary code on the vulnerable systems.	No	Yes	FALSE
CVE-2021-20123	Draytek	VigorConnect	An unauthenticated local file inclusion vulnerability DownloadFileServlet endpoint in that enables an unauthenticated attacker to download arbitrary files with root privileges	No	Yes	FALSE
CVE-2021-20124	Draytek	VigorConnect	An unauthenticated local file inclusion vulnerability WebServlet endpoint that enables an unauthenticated attacker to download arbitrary files with root privileges.	No	Yes	FALSE
CVE-2021-4043	GPAC Development Team	GPAC	A null pointer dereference vulnerability in the Motion Spell GitHub repository GPAC that can be exploited to execute arbitrary code.	No	Yes	TRUE
CVE-2020-0618	Microsoft	SQL Server Reporting Services	A remote code execution vulnerability in the Microsoft SQL Server that can enable an attacker to execute arbitrary code in the context of Report Server service account.	Yes	Yes	FALSE

CVE-ID	Vendor	Product	Description	Abused by malware	CISA KEV	OSS
CVE-2020-14644	Oracle	WebLogic Server	A remote code execution vulnerability in the Oracle WebLogic Server that enables the attacker to gain complete control over the affected system.	No	Yes	FALSE
CVE-2020-15415	DrayTek	Vigor router	An OS command injection vulnerability in the DrayTek Vigor router that enables unauthenticated attackers to execute malicious code on the vulnerable systems.	Yes	Yes	FALSE
CVE-2019-1069	Microsoft	Windows Task scheduler	An elevation of privilege vulnerability in the Windows task scheduler.	Yes	Yes	FALSE
CVE-2019-0344	SAP SE	Commerce Cloud	Deserialization of Untrusted Data Vulnerability AP Commerce Cloud allows attackers to execute malicious code on a target system by exploiting the unsafe deserialization process.	No	Yes	FALSE
CVE-2017-1000253	The Linux Foundation	Linux Kernel	A stack-based buffer overflow vulnerability in the Linux Kernel that enables a local attacker to escalate privileges.	Yes	Yes	FALSE
CVE-2016-3714	ImageMagick Studio LLC	ImageMagick	An improper input validation vulnerability in the ImageMagick that enables an attacker to execute arbitrary code by crafting an image with malicious shell metacharacters.	No	Yes	TRUE
CVE-2014-0497	Adobe	Flash Player	An integral underflow vulnerability in the Adobe Flash Player that enables remote attackers to execute arbitrary code on the vulnerable systems.	Yes	Yes	FALSE
CVE-2014-0502	Adobe	Flash Player	A double free vulnerability in Adobe Flash Player that enables remote attackers to execute arbitrary code on the vulnerable systems.	Yes	Yes	FALSE
CVE-2013-0643	Adobe	Flash Player	An incorrect default permissions vulnerability in the Adobe Flash player that enables a remote attacker to execute arbitrary code on the vulnerable systems.	No	Yes	FALSE
CVE-2013-0648	Adobe	Flash Player	A remote code execution vulnerability in the Adobe Flash player that can enable remote attackers to execute arbitrary code on vulnerable systems.	No	Yes	FALSE

October

In October, 22 vulnerabilities were actively exploited, with 17 added to the CISA KEV catalog. These included four Microsoft vulnerabilities, three Ivanti vulnerabilities, and two Fortinet vulnerabilities. Notably, eight zero-day vulnerabilities were actively exploited, with Microsoft and Ivanti accounting for three each. Among the attack types, six involved Remote Code Execution (RCE), three were use-after-free vulnerabilities, and two were related to deserialization flaws.

CVE-ID	Vendor	Product	Description	Abused by malware	CISA KEV	OSS
CVE-2024-29824	Ivanti	Endpoint Manager (EPM)	A SQL injection vulnerability in Ivanti EPM allows unauthenticated attackers within the same network to execute malicious code on unpatched systems.	No	Yes	FALSE
CVE-2024-45519	Synacor	Zimbra Collaboration Suite (ZCS)	A remote code execution vulnerability in Zimbra's postjournal service that could enable unauthenticated threat actors to execute arbitrary commands on the vulnerable systems.	No	Yes	FALSE
CVE-2024-43047	Qualcomm	Multiple Chipsets	A use after free vulnerability in the Qualcomm Digital Signal Processor (DSP) service.	No	Yes	FALSE
CVE-2024-43572	Microsoft	Management Console	A remote code execution vulnerability in Microsoft Management Console (MMC) that can be exploited by tricking users into opening a malicious file, often through social engineering techniques.	No	Yes	FALSE
CVE-2024-43573	Microsoft	Windows MSHTML Platform	A spoofing vulnerability in the Windows MSHTML Platform	No	Yes	FALSE
CVE-2024-9379	Ivanti	Cloud Service Appliance (CSA)	A SQL injection vulnerability in the Ivanti CSA admin web console allows a remote, authenticated attacker with administrator privileges to execute arbitrary SQL commands.	No	Yes	FALSE
CVE-2024-9380	Ivanti	Cloud Service Appliance	A command injection vulnerability in the Ivanti CSA admin web console could allow a remote, authenticated attacker with administrator privileges to execute arbitrary commands on the system.	No	Yes	FALSE
CVE-2024-9381	Ivanti	Cloud Service Appliance	A path traversal vulnerability in Ivanti CSA could allow a remote, authenticated attacker with administrator privileges to bypass security restrictions.	No	No	FALSE
CVE-2024-23113	Fortinet	FortiOS	A critical remote code execution vulnerability in Fortinet FortiOS allows unauthenticated attackers to execute commands on vulnerable devices without requiring any user interaction.	No	Yes	FALSE
CVE-2024-30088	Microsoft	Windows Kernel	A privilege escalation vulnerability in the Windows kernel could allow attackers to elevate their privileges to SYSTEM level, granting them significant control over compromised devices.	Yes	Yes	FALSE
CVE-2024-9680	Mozilla Corporation	Firefox and Thunderbird	A use-after-free vulnerability in the Animation timeline component of Mozilla Firefox.	No	Yes	FALSE
CVE-2024-28987	SolarWinds	Web Help Desk (WHD)	Critical hardcoded credential vulnerability in the SolarWinds Web Help Desk (WHD) software that enables remote unauthenticated users to access internal functionality and modify data.	No	Yes	FALSE
CVE-2024-40711	Veeam Software	Backup & Replication	A deserialization of untrusted data vulnerability in Veeam Backup & Replication that allows for unauthenticated remote code execution	Yes	Yes	FALSE
CVE-2024-38178	Microsoft	Internet Explorer (IE)	A memory corruption vulnerability in the scripting engine that could lead to remote code execution when using the Edge browser in Internet Explorer mode.	Yes	Yes	FALSE
CVE-2024-44133	Apple	macOS	A vulnerability in macOS, referred to as "HM Surf," enables attackers to circumvent the operating system's Transparency, Consent, and Control (TCC) technology, allowing them unauthorized access to a user's protected data.	Yes	No	FALSE

CVE-ID	Vendor	Product	Description	Abused by malware	CISA KEV	OSS
CVE-2024-9537	ScienceLogic	SL1	A remote code execution vulnerability in the ScienceLogic SL1 platform could allow unauthorized access to its internal performance reporting systems.	Yes	Yes	FALSE
CVE-2024-37383	Roundcube	Webmail	A stored cross-site scripting (XSS) vulnerability has been identified in Roundcube Webmail, which can be exploited via SVG animate attributes.	Yes	Yes	TRUE
CVE-2024-38094	Microsoft	SharePoint server	A deserialization vulnerability in Microsoft SharePoint allows attackers to potentially execute arbitrary commands on affected systems.	No	Yes	FALSE
CVE-2024-44068	Samsung	Mobile Processor	A use-after-free vulnerability in the Samsung Mobile Processor that can lead to privilege escalation	No	No	FALSE
CVE-2024-20481	Cisco	Adaptive Security Appliance and Firepower Threat Defense (FTD)	A vulnerability in the Remote Access VPN (RAVPN) service of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could enable an unauthenticated remote attacker to trigger a denial-of-service (DoS) attack	No	Yes	FALSE
CVE-2024-47575	Fortinet	FortiManager	A missing authentication vulnerability in the Fortinet FortiManager fgfmd daemon could allow a remote, unauthenticated attacker to execute arbitrary code or commands by sending specially crafted requests	Yes	Yes	FALSE
CVE-2017-0144	Microsoft	Server Message Block (SMB) protocol	A remote code execution vulnerability in the Microsoft Server Message Block (SMB) server could be exploited by an attacker to execute arbitrary code on a targeted server, potentially granting them control over the system	Yes	Yes	FALSE

login:soft

November

In November 2024, 42 vulnerabilities were actively exploited, with 22 added to the CISA Known Exploited Vulnerabilities (KEV) catalog. These included five affecting Palo Alto Networks, two each for Microsoft, Apple, PTZOptics, and VMware vCenter Server. The attack types comprised eleven Remote Code Executions (RCE), seven command injection flaws, five authentication bypasses, and three elevation of privilege vulnerabilities. Notably, eight were zero-day exploits, underscoring the critical need for organizations to prioritize timely patches and enhance security measures.

CVE-ID	Vendor	Product	Description	Abused by malware	CISA KEV	OSS
CVE-2024-8956	PTZOptics	PT30X-SDI/NDI Cameras	An authentication bypass vulnerability could allow attackers to gain unauthorized access to the camera's administrative interface without needing valid credentials, effectively bypassing security controls.	No	Yes	FALSE
CVE-2024-8957	PTZOptics	PT30X-SDI/NDI Cameras	A command injection vulnerability may allow attackers to execute arbitrary commands, potentially granting them full control over the affected system.	No	Yes	FALSE
CVE-2024-43093	Google	Android Framework Component	An elevation of privilege vulnerability could enable attackers to gain unauthorized access and perform actions with higher-level privileges than intended.	No	Yes	TRUE
CVE-2024-5910	Palo Alto Networks	Expedition	A critical authentication flaw could enable attackers with network access to compromise an administrator account, granting them full control over the system.	No	Yes	FALSE
CVE-2024-4577	The PHP Group	PHP	A critical argument injection vulnerability that can be leveraged to achieve remote code execution.	Yes	Yes	FALSE
CVE-2024-49039	Microsoft	Windows	An Elevation of Privilege vulnerability in the Windows task scheduler	No	Yes	FALSE
CVE-2024-43451	Microsoft	Windows	Windows NTLM has disclosure spoofing vulnerability.	Yes	Yes	FALSE
CVE-2024-10914	D-Link	NAS	A command injection vulnerability that allows unauthenticated attackers to inject arbitrary shell commands via specially crafted HTTP GET requests.	No	No	FALSE
CVE-2024-9463	Palo Alto Networks	Expedition	An unauthenticated OS command injection vulnerability in the Palo Alto Networks Expedition	No	Yes	FALSE
CVE-2024-9465	Palo Alto Networks	Expedition	An unauthenticated SQL injection vulnerability in the Palo Alto Expedition	No	Yes	FALSE
CVE-2024-0012	Palo Alto Networks	PAN-OS software	An authentication bypass vulnerability in PAN-OS allows unauthenticated attackers with network access to the management web interface to escalate privileges to administrator level.	Yes	Yes	FALSE
CVE-2024-9474	Palo Alto Networks	PAN-OS software	An OS command injection vulnerability allows administrators with access to the management web interface to escalate their privileges and execute actions on the firewall with root-level permissions	No	Yes	FALSE
CVE-2024-11120	GeoVision	Devices	A pre-authentication command injection vulnerability in the GeoVision	Yes	No	FALSE
CVE-2024-11680	ProjectSend	ProjectSend	An improper authentication vulnerability allows remote, unauthenticated attackers to exploit the issue by sending specially crafted HTTP requests to the application's configuration	No	No	FALSE
CVE-2024-11667	Zyxel	Firewall models	A directory traversal vulnerability identified in the web management interface of Zyxel ZLD firewall firmware	Yes	No	FALSE
CVE-2024-1212	Progress Software Corporation	Kemp LoadMaster	A command injection vulnerability in the Kemp LoadMaster allows unauthenticated attackers to gain access to the LoadMaster management interface, potentially compromising the system's integrity and security.	No	Yes	FALSE
CVE-2024-8068	Citrix	Session Recording	Privilege escalation to Network Service Account access in Citrix Session Recording	No	No	FALSE

CVE-ID	Vendor	Product	Description	Abused by malware	CISA KEV	OSS
CVE-2024-8069	Citrix	Session Recording	Limited remote code execution with privilege of a Network Service Account access	No	No	FALSE
CVE-2024-38812	VMware	vCenter Server	A heap overflow vulnerability allows a malicious actor with network access to send specially crafted packets, potentially resulting in remote code execution.	No	Yes	FALSE
CVE-2024-38813	VMware	vCenter Server	A privilege escalation vulnerability allows an attacker with network access to gain root privileges by sending a specially crafted network packet.	No	Yes	FALSE
CVE-2024-44308	Apple	Multiple products	A vulnerability in JavaScriptCore could allow arbitrary code execution when processing maliciously crafted web content.	No	Yes	FALSE
CVE-2024-44309	Apple	Multiple products	Cookie management vulnerability in WebKit could enable cross-site scripting (XSS) attacks when handling specially crafted malicious web content, potentially compromising user data and security.	No	Yes	FALSE
CVE-2024-21287	Oracle	Agile PLM Framework	An incorrect authorization vulnerability that could be exploited remotely without requiring any authentication.	No	Yes	FALSE
CVE-2024-42057	Zyxel	Firewall models	A command injection vulnerability in the IPsec VPN feature of certain firewall versions enables unauthenticated attackers to execute arbitrary OS commands. This can be exploited by sending a specially crafted username to the vulnerable device, potentially compromising its integrity.	Yes	No	FALSE
CVE-2023-1389	TP-Link	Archer AX21 (AX1800)	A command injection vulnerability exists in the country form of the <code>/cgi-bin/luci;stok=/locale</code> endpoint on the web management interface, potentially allowing attackers to execute unauthorized commands.	Yes	Yes	FALSE
CVE-2023-28461	Array Networks	AG and vxAG ArrayOS	An improper authentication vulnerability that could be exploited remotely, potentially allowing attackers to execute arbitrary code on the affected systems	Yes	Yes	FALSE
CVE-2022-1040	Sophos	Firewall	An authentication bypass vulnerability specifically in the User Portal and Webadmin components, that allows remote attackers to execute arbitrary code.	Yes	Yes	FALSE
CVE-2022-21587	Oracle	E-Business Suite	An unauthenticated remote code execution vulnerability in the Oracle E-Business Suite that allows unauthenticated attackers to remotely upload malicious files via HTTP, potentially leading to full control over the affected application.	Yes	Yes	FALSE
CVE-2021-41773	Apache	HTTP	A path traversal vulnerability that allows an attacker with network access to use a crafted URL path to map and access files outside of the server's document root, effectively bypassing security controls.	Yes	Yes	FALSE
CVE-2021-26086	Atlassian	Confluence Server and Data Center	A remote code execution vulnerability in the Questions for Confluence app within the Atlassian's Confluence Server and Data Center products where improper permissions handling could allow an unauthenticated attacker to execute arbitrary code on the server.	Yes	Yes	FALSE
CVE-2021-41277	Metabase	Metabase	A vulnerability in Metabase, an open-source business intelligence tool, allows attackers to exploit a Local File Inclusion (LFI) issue within its custom GeoJSON map functionality.	Yes	Yes	FALSE
CVE-2021-41285	Crucial by Micron Technology, Inc.	Ballistix MOD Utility	A local privilege escalation vulnerability in the MODAPI.sys driver allows low-privileged users to leverage the MmMapIoSpace function to access physical memory, potentially leading to unauthorized access and system compromise.	Yes	No	FALSE

CVE-ID	Vendor	Product	Description	Abused by malware	CISA KEV	OSS
CVE-2020-1472	Microsoft	Windows Server versions with Active Directory	This vulnerability, also known as "ZeroLogon," is a critical security vulnerability that affects Windows Server operating systems and was disclosed by Microsoft in August 2020.	Yes	Yes	TRUE
CVE-2020-14979	OpenLibSys	WinRing0.sys and WinRing0x64.sys drivers	A local privilege escalation vulnerability in the WinRing0_1_2_0 driver service allows low-privileged users or attackers to execute arbitrary commands with SYSTEM-level privileges, posing a significant risk to system integrity and security.	Yes	No	FALSE
CVE-2019-16278	Nostromo	nhttpd	A directory traversal vulnerability allows attackers to access directories outside the intended scope, potentially leading to unauthorized command execution and posing a significant risk for remote code execution.	No	Yes	FALSE
CVE-2018-15133	Laravel	Framework	A vulnerability that enables remote attackers to execute arbitrary code on affected systems by exploiting an unserialization flaw within the framework's encryption mechanism.	Yes	Yes	TRUE
CVE-2018-10561	Dasan Networks	GPON home routers	Authentication bypass vulnerability in the DASAN GPON home routers.	Yes	Yes	FALSE
CVE-2018-10562	Dasan Networks	GPON home routers	Command injection vulnerability in the DASAN GPON home routers.	Yes	Yes	FALSE
CVE-2017-9841	PHPUnit Development Team	PHPUnit	A vulnerability in the PHPUnit which is caused due to improper input validation within the framework's PHPUnit\Util\PHP file, which can allow an attacker to achieve remote code execution on the affected system.	Yes	Yes	TRUE
CVE-2017-0199	Microsoft	Office and WordPad	A remote code execution vulnerability in Microsoft Office and WordPad that can be leveraged by an attacker to take complete control of the affected system.	Yes	Yes	FALSE
CVE-2014-2120	Cisco	Adaptive Security Appliance (ASA)	A cross-site scripting (XSS) vulnerability in the WebVPN login page of Cisco Adaptive Security Appliance (ASA) software that allows remote attackers to inject arbitrary webscript or HTML code via an unspecified parameter.	Yes	Yes	FALSE

December

In December 2024, 27 vulnerabilities were actively exploited, with 16 added to CISA's Known Exploited Vulnerabilities (KEV) catalog. These included two vulnerabilities each in Microsoft products, Reolink devices, NUUO NVRmini devices, and Cleo multiple products. The attack types comprised seven Remote Code Execution (RCE) vulnerabilities, four command injection vulnerabilities, two traversal vulnerabilities, two improper access control vulnerabilities, one elevation of privilege (EOP) vulnerability, and one denial-of-service (DoS) vulnerability.

CVE-ID	Vendor	Product	Description	Abused by malware	CISA KEV	OSS
CVE-2024-12856	Four-Faith	Industrial routers	An unauthenticated operating system command injection vulnerability in the Four-Faith industrial routers that allows attackers to execute arbitrary commands on vulnerable devices remotely.	No	No	FALSE
CVE-2024-12356	BeyondTrust	Privileged Remote Access (PRA) and Remote Support (RS)	A command injection vulnerability in BeyondTrust's Privileged Remote Access (PRA) and Remote Support (RS) products could enable an unauthenticated attacker to inject malicious commands.	No	Yes	FALSE
CVE-2024-55956	Cleo	Harmony, VLTrader, and LexiCom	An unrestricted file upload vulnerability allows an unauthenticated attacker to import and execute arbitrary Bash or PowerShell commands on the host system by exploiting the default settings of the Autorun directory.	Yes	Yes	FALSE
CVE-2024-50623	Cleo	Harmony, VLTrader, and LexiCom	An unrestricted file upload and download vulnerability that can be exploited to achieve remote code execution with elevated privileges.	Yes	Yes	FALSE
CVE-2024-35250	Microsoft	Windows	A vulnerability in the Microsoft Windows Kernel-mode Driver involving an untrusted pointer dereference could allow attackers to execute malicious code with elevated system privileges upon successful exploitation.	No	Yes	FALSE
CVE-2024-49035	Microsoft	Partner Center	An improper access control vulnerability in the partner.microsoft[.]complatform enables an unauthenticated attacker to perform privilege escalation over a network, potentially compromising sensitive operations and data.	No	No	FALSE
CVE-2024-20767	Adobe	ColdFusion	An improper access control vulnerability in Adobe ColdFusion allows attackers to access or modify restricted files, potentially compromising sensitive information.	No	Yes	FALSE
CVE-2024-49138	Microsoft	Windows	An Elevation of Privilege vulnerability in the Windows Common Log File System (CLFS) Driver	No	Yes	FALSE
CVE-2024-51378	CyberPanel	CyberPanel	An incorrect default permissions vulnerability enables authentication bypass and allows the execution of arbitrary commands by exploiting shell metacharacters in the statusfile property.	Yes	Yes	FALSE
CVE-2024-11680	ProjectSend	ProjectSend	An improper authentication vulnerability allows remote, unauthenticated attackers to exploit the issue by sending specially crafted HTTP requests to the application's configuration.	No	Yes	FALSE
CVE-2024-11667	Zyxel	Multiple Firewalls	A directory traversal vulnerability identified in the web management interface of Zyxel ZLD firewall firmware.	Yes	Yes	FALSE
CVE-2024-45841	I-O DATA DEVICE	UD-LT1 and UD-LT1/EX routers	An attacker with access to a guest account could exploit this vulnerability to capture and potentially steal user credentials.	No	No	FALSE

CVE-ID	Vendor	Product	Description	Abused by malware	CISA KEV	OSS
CVE-2024-47133	I-O DATA DEVICE	UD-LT1 and UD-LT1/EX routers	This vulnerability enables an authenticated administrator to execute arbitrary operating system commands, potentially allowing attackers to gain complete control over the device.	No	No	FALSE
CVE-2024-52564	I-O DATA DEVICE	UD-LT1 and UD-LT1/EX routers	A remote attacker could exploit this vulnerability to disable the firewall functionality of affected devices.	No	No	FALSE
CVE-2024-11972	Hunk Themes	Hunk Companion WordPress Plugin	A vulnerability allowing the arbitrary installation of plugins via unauthenticated POST requests.	No	No	FALSE
CVE-2024-53677	Apache	Struts	A remote code execution vulnerability has been identified, allowing attackers to execute arbitrary code by exploiting weaknesses in the file upload mechanism.	No	No	FALSE
CVE-2024-41713	Mitel	MiCollab	A path traversal vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab that arises due to insufficient input validation.	No	No	FALSE
CVE-2024-35286	Mitel	MiCollab	A pre-authentication SQL injection vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab allows attackers to execute unauthorized database operations, potentially compromising sensitive information.	No	No	FALSE
CVE-2024-3393	Palo Alto Networks	PAN-OS	A denial-of-service (DoS) vulnerability has been identified in the DNS Security feature of Palo Alto Networks' PAN-OS software.	Yes	No	FALSE
CVE-2024-33112	D-Link	DIR-845L	A command injection vulnerability has been identified in D-Link DIR routers through the hnap_main() function.	Yes	No	FALSE
CVE-2023-46604	Apache	ActiveMQ server	A remote execution vulnerability in the Apache ActiveMQ server, that can allow an attacker to execute malicious commands remotely and take complete control over the target system.	Yes	Yes	TRUE
CVE-2023-45727	North Grid	Proself	This vulnerability enables remote, unauthenticated attackers to execute XML External Entity (XXE) attacks. By sending a specially crafted XML request, the attacker can access and potentially read sensitive files stored on the server, including private account information	Yes	Yes	FALSE
CVE-2022-23227	NUUO	NVRmini 2 Devices	A missing authentication vulnerability in the NUUO NVRmini 2 devices.	No	Yes	FALSE
CVE-2021-40407	Reolink	RLC-410W IP Camera	An OS command injection vulnerability in the ReoLink IP camera.	No	Yes	FALSE
CVE-2021-44207	Acclaim Systems	USAHERDS	Use of Hard-Coded credentials vulnerability in the Acclaim Systems USAHERDS that could result in an arbitrary code execution on the susceptible servers	Yes	Yes	FALSE
CVE-2019-11001	Reolink	Multiple IP Cameras	An OS command injection vulnerability in Reolink Multiple IP cameras.	No	Yes	FALSE
CVE-2018-14933	NUUO	NVRmini Devices	An OS command injection vulnerability in the NUUO NVRmini Devices.	No	Yes	FALSE

Sources Cited

1. <https://www.cisa.gov/news-events/alerts/2024/01/10/cisa-adds-two-known-exploited-vulnerabilities-catalog>
2. <https://www.cisa.gov/news-events/alerts/2024/01/31/cisa-adds-one-known-exploited-vulnerability-catalog-0>
3. <https://www.cisa.gov/news-events/alerts/2024/01/17/cisa-adds-three-known-exploited-vulnerabilities-catalog>
4. <https://www.cisa.gov/news-events/alerts/2024/01/23/cisa-adds-one-known-exploited-vulnerability-catalog>
5. <https://www.cisa.gov/news-events/alerts/2024/01/24/cisa-adds-one-known-exploited-vulnerability-catalog>
6. <https://www.cisa.gov/news-events/alerts/2024/02/15/cisa-adds-two-known-exploited-vulnerabilities-catalog>
7. <https://www.cisa.gov/news-events/alerts/2024/02/13/cisa-adds-two-known-exploited-vulnerabilities-catalog>
8. <https://www.cisa.gov/news-events/alerts/2024/02/09/cisa-adds-one-known-exploited-vulnerability-catalog>
9. <https://www.cisa.gov/news-events/alerts/2024/02/29/cisa-adds-one-known-exploited-vulnerability-catalog>
10. <https://www.cisa.gov/news-events/alerts/2024/02/06/cisa-adds-one-known-exploited-vulnerability-catalog>
11. <https://www.cisa.gov/news-events/alerts/2024/03/04/cisa-adds-one-known-exploited-vulnerability-catalog>
12. <https://www.cisa.gov/news-events/alerts/2024/03/06/cisa-adds-two-known-exploited-vulnerabilities-catalog>
13. <https://www.cisa.gov/news-events/alerts/2024/03/26/cisa-adds-one-known-exploited-vulnerability-catalog>
14. <https://www.cisa.gov/news-events/alerts/2024/03/25/cisa-adds-three-known-exploited-vulnerabilities-catalog>
15. <https://www.cisa.gov/news-events/alerts/2024/03/05/cisa-adds-two-known-exploited-vulnerabilities-catalog>
16. <https://www.cisa.gov/news-events/alerts/2024/04/30/cisa-adds-one-known-exploited-vulnerability-catalog>
17. <https://www.cisa.gov/news-events/alerts/2024/04/24/cisa-adds-three-known-exploited-vulnerabilities-catalog>
18. <https://www.cisa.gov/news-events/alerts/2024/04/04/cisa-adds-two-known-exploited-vulnerabilities-catalog>
19. <https://www.cisa.gov/news-events/alerts/2024/04/23/cisa-adds-one-known-exploited-vulnerability-catalog>
20. <https://www.cisa.gov/news-events/alerts/2024/05/13/cisa-adds-one-known-exploited-vulnerability-catalog>
21. <https://www.cisa.gov/news-events/alerts/2024/05/20/cisa-adds-two-known-exploited-vulnerabilities-catalog>
22. <https://www.cisa.gov/news-events/alerts/2024/05/16/cisa-adds-three-known-exploited-vulnerabilities-catalog>
23. <https://www.cisa.gov/news-events/alerts/2024/05/28/cisa-adds-one-known-exploited-vulnerability-catalog>
24. <https://www.cisa.gov/news-events/alerts/2024/05/14/cisa-adds-two-known-exploited-vulnerabilities-catalog>
25. <https://www.cisa.gov/news-events/alerts/2024/05/01/cisa-adds-one-known-exploited-vulnerability-catalog>
26. <https://www.cisa.gov/news-events/alerts/2024/07/30/cisa-adds-one-known-exploited-vulnerability-catalog>

27. <https://www.cisa.gov/news-events/alerts/2024/08/26/cisa-adds-one-known-exploited-vulnerability-catalog>
28. <https://www.cisa.gov/news-events/alerts/2024/08/28/cisa-adds-one-known-exploited-vulnerability-catalog>
29. <https://www.cisa.gov/news-events/alerts/2024/08/07/cisa-adds-two-known-exploited-vulnerabilities-catalog>
30. <https://www.cisa.gov/news-events/alerts/2024/08/27/cisa-adds-one-known-exploited-vulnerability-catalog>
31. <https://www.alphatechs.al/post/new-mirai-variants-targeting-latest-vulnerabilities-in-iot-devices>
32. <https://www.akamai.com/blog/security-research/2024-php-exploit-cve-one-day-after-disclosure>
33. <https://www.fortinet.com/blog/threat-research/Iz1h9-campaign-enhances-arsenal-with-scores-of-exploits>
34. <https://www.imperva.com/blog/new-sysrv-botnet-variant-makes-use-of-google-subdomain-to-spread-xmrig-miner/>
35. <https://unit42.paloaltonetworks.com/cve-2022-22954-vmware-vulnerabilities/>
36. <https://vulncheck.com/blog/moobot-uses-fake-vulnerability>
37. <https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/>
38. <https://www.cloudsek.com/blog/major-payment-disruption-ransomware-strikes-indian-banking-infrastructure>
39. <https://www.scmagazine.com/brief/new-shadowsyndicate-ransomware-attacks-involve-aiohttp-flaw-exploitation>
40. <https://asec.ahnlab.com/en/85000/>
41. <https://labs.withsecure.com/publications/new-krustyloder-variant-dropped-via-screenconnect-exploit>
42. https://www.csk.gov.in/alerts/STOP_ransomware.html
43. <https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/>
44. <https://www.zdnet.com/article/almost-one-million-windows-systems-vulnerable-to-bluekeep-cve-2019-0708/>
45. <https://www.redpacketsecurity.com/lemonduck-no-longer-settles-for-breadcrumbs/>
46. https://www.hivepro.com/wp-content/uploads/2023/10/In-Depth-Analysis-of-Phobos-Ransomware_TA2023426-Updated.pdf
47. <https://sensorstechforum.com/cve-2017-0213-dharma-ransomware/>
48. <https://www.fortinet.com/blog/threat-research/sophisticated-attack-targets-taiwan-with-smokeloder>
49. <https://www.programmersought.com/article/62493896999/>
50. <https://blog.morphisec.com/iranian-fileless-cyberattack-on-israel-word-vulnerability>
51. <https://www.fortinet.com/blog/threat-research/new-campaign-uses-remcos-rat-to-exploit-victims>
52. <https://nsfocusglobal.com/satan-variant-analysis-handling-guide/>
53. <https://blogs.juniper.net/en-us/threat-research/cve-2024-23897-enabled-ransomware-attack-on-indian-banks>
54. <https://cloud.google.com/blog/topics/threat-intelligence/investigating-ivanti-zero-day-exploitation/>
55. <https://www.cloudsek.com/blog/mozi-resurfaces-as-androxgh0st-botnet-unraveling-the-latest-exploitation-wave>
56. <https://www.akamai.com/blog/security-research/2024-corona-mirai-botnet-infects-zero-day-sirt>
57. <https://asec.ahnlab.com/en/85000/>
58. <https://securelist.com/elpaco-ransomware-a-mimic-variant/114635/>
59. <https://www.barracuda.com/company/legal/esg-vulnerability>
60. <https://cloud.google.com/blog/topics/threat-intelligence/chinese-vmware-exploitation-since-2021/>
61. <https://symantec-enterprise-blogs.security.com/threat-intelligence/black-basta-ransomware-zero-day>
62. https://www.theregister.com/2024/06/24/mirailike_botnet_zyxel_nas/
63. https://www.trendmicro.com/en_us/research/24/e/decoding-8220-latest-obfuscation-tricks.html
64. <https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations>
65. <https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware>
66. <https://securelist.com/elpaco-ransomware-a-mimic-variant/114635/>
67. <https://www.group-ib.com/blog/estate-ransomware/>

68. <https://www.scworld.com/news/open-source-ransomware-rats-deployed-on-compromised-teamcity-servers>
69. <https://www.sangfor.com/farsight-labs-threat-intelligence/cybersecurity/bablock-rorschach-ransomware>
70. <https://www.trellix.com/blogs/research/cactus-ransomware-new-strain-in-the-market/>
71. <https://news.sophos.com/en-us/2024/11/08/veeam-exploit-seen-used-again-with-a-new-ransomware-frag/>
72. <https://censys.com/cve-2024-51378/>
73. <https://arcticwolf.com/resources/blog/arctic-wolf-labs-observes-increased-fog-and-akira-ransomware-activity-linked-to-sonicwall-ssl-vpn/>
74. <https://socprime.com/blog/zola-ransomware-detection-proton-family-evolves-with-a-new-ransomware-variant-featuring-a-kill-switch/>
75. <https://otx.alienvault.com/pulse/6761a75807a4d64dc1d8a3d4>
76. <https://www.sentinelone.com/anthology/inc-ransom/>
77. <https://www.secureworks.com/blog/gold-ionic-deploys-inc-ransomware>
78. <https://medium.com/@brotheralameen/malware-analysis-of-noescape-ransomware-56365f8d33ec>
79. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
80. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a>
81. <https://blog.darklab.hk/tag/cve-2019-7481/>
82. <https://www.securin.io/articles/all-about-lockbit-ransomware/>
83. <https://socradar.io/dark-web-profile-play-ransomware/>
84. <https://www.fortiguard.com/threat-signal-report/4927/new-exploit-method-bypasses-official-proxynotshell-mitigation>
85. <https://arcticwolf.com/resources/blog/arctic-wolf-observes-akira-ransomware-campaign-targeting-sonicwall-sslvpn-accounts/>
86. <https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/>
87. <https://blog.qualys.com/vulnerabilities-threat-research/2024/10/02/threat-brief-understanding-akira-ransomware>
88. https://www.theregister.com/AMP/2024/07/30/make_me_admin_esxi_flaw/
89. <https://cybersrcc.com/2024/06/15/black-basta-ransomware-may-have-exploited-ms-windows-zero-day-flaw/>
90. <https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/>
91. <https://socradar.io/threat-actor-profile-bianlian-the-shape-shifting-ransomware-group/>
92. <https://www.reliaquest.com/blog/inc-ransom-attack-analysis/>
93. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a>
94. <https://www.guidedpointsecurity.com/blog/bianlian-gos-for-powershell-after-teamcity-exploitation/>
95. <https://www.logpoint.com/en/blog/emerging-threat/bianlian-ransomware/>
96. <https://www.trendmicro.com/vinfo/hk-en/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta>
97. <https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/>
98. <https://www.picussecurity.com/resource/blog/cisa-alert-aa23-131a-bl00dy-ransomware-exploits-paper-cut-cve-2023-27350-vulnerability>
99. <https://www.jetir.org/papers/JETIR2401399.pdf>

Conclusion

As the threat landscape continues to evolve, organizations must prioritize timely patching and implement robust defenses to mitigate risks effectively. Loginsoft Vulnerability Intelligence (LOVI) empowers organizations to stay ahead of emerging threats by providing real-time sensor intelligence, detailed threat profiles, and insights into trending vulnerabilities and Ransomware tactics. By addressing vulnerabilities before they escalate into critical threats, our advanced solutions enable organizations to secure their systems and build resilience for the future. With a proactive approach to cybersecurity, LOVI ensures that your organization remains protected in an increasingly complex threat environment.



About Loginsoft

As a leading cybersecurity research company, Loginsoft has been providing innovative and customized solutions to clients since its establishment in 2005. Headquartered in Virginia, USA, the company specializes in information technology consulting and services, offering expertise in cyber threat intelligence, threat hunting, vulnerability research, and software supply-chain security research. With a commitment to staying at the forefront of cybersecurity research, Loginsoft is dedicated to helping clients stay protected from the ever-evolving landscape of cyber threats. Additionally, Loginsoft offers a unique research-as-a-service approach, providing clients with tailored solutions to their specific cybersecurity needs. Trust Loginsoft to safeguard your organization and stay ahead of potential cyber threats.



To learn more, visit 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