loginsoft

Monthly Report

Threat & Vulnerabilities Report – February 2025

Executive Summary

February 2025 saw a significant surge in newly added vulnerabilities to the CISA Known Exploited Vulnerabilities (KEV) catalog, highlighting increased adversary focus on both newly discovered and legacy flaws across critical software, devices, and open-source platforms. Notably, over 27 vulnerabilities were added to KEV across vendors such as Microsoft, Palo Alto Networks, Apple, Zyxel, and PostgreSQL, with several vulnerabilities exploited as zero-days and some actively abused by malware in ongoing campaigns. The targeted vulnerabilities range from authentication bypass and remote code execution to privilege escalation and command injection, impacting network devices, enterprise applications, and consumer platforms alike. This rapid expansion of the KEV list underscores the urgent need for organizations to prioritize timely patching, enhance detection capabilities, and monitor emerging threats to mitigate evolving exploitation tactics and protect critical assets.

In addition, 15 vulnerabilities were exploited as zero-days in February 2025, underscoring the growing risk from threat actors leveraging unpatched and previously unknown security flaws.

Ransomware groups Clop, Ransomhub and Akira made their presence felt in February 2025, compromising major sectors like healthcare, finance, and manufacturing, underscoring the escalating risk to critical industries.

Actively Exploited Vulnerabilities

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	CISA KEV	OSS
CVE-2025-0111	Palo Alto Networks	PAN-OS Software	A File Read Vulnerability in the Palo Alto Networks PAN-OS Software	No	No	Yes	False
CVE-2025-0108	Palo Alto Networks	PAN-OS Software	An Authentication Bypass Vulnerability in the Palo Alto Networks PAN-OS software	No	No	No	False

CVE-2025-0411	7-Zip	7-Zip	A Mark-of-the-Web Bypass Vulnerability in 7-Zip allows remote attackers to execute arbitrary code with the privileges of the current user	Yes	Yes	Yes	False
CVE-2025-0890	Zyxel	CPE Devices	A Default Credentials Vulnerability in Zyxel CPE devices	Yes	No	No	False
CVE-2025-0994	Trimble	Cityworks	Deserialization of Untrusted Data Vulnerability in Trimble Cityworks could allow an attacker to execute remote code on the targeted system	Yes	No	Yes	False
CVE-2025-1094	PostgreSQL	psql	An SQL Injection Vulnerability in the PostgreSQL interactive tool psql	Yes	Yes	No	False
CVE-2025-21391	Microsoft	Windows	A Link Following Vulnerability in the Microsoft Windows Storage, which could enable privilege escalation, allowing attackers to gain elevated system privileges	Yes	No	Yes	False

CVE-2025-21418	Microsoft	Windows	A Heap-Based Buffer Overflow Vulnerability in the Microsoft Windows Ancillary Function Driver for WinSock	Yes	No	Yes	False
CVE-2025-23209	Craft CMS	Craft CMS	A Code Injection Vulnerability in the Craft CMS can lead to unauthorized access and system takeover	No	No	Yes	True
CVE-2025-24200	Apple	IOS and iPadOS	An Improper Authorization Vulnerability in the Apple iPadOS and iOS	Yes	No	Yes	False
CVE-2025-24989	Microsoft	Power Pages	An Elevation of Privilege Vulnerability in the Microsoft Power Pages	Yes	No	Yes	False
CVE-2025-25181	Advantive	VeraCore	An SQL Injection Vulnerability in Advantive VeraCore enables remote attackers to execute arbitrary SQL commands, potentially compromising the database and exposing sensitive information	Yes	Yes	No	False
CVE-2024-20953	Oracle	Agile Product Lifecycle Management (PLM)	A Deserializatio n Vulnerability in the Oracle	No	No	Yes	False

			Agile Product Lifecycle Management (PLM)				
CVE-2024-21413	Microsoft	Outlook	A Remote Code Execution Vulnerability in Microsoft Outlook	Yes	Yes	Yes	False
CVE-2024-29059	Microsoft	.NET Framework	An Information Disclosure Vulnerability in the Microsoft .NET framework	No	No	Yes	False
CVE-2024-38213	Microsoft	Windows	Security Feature Bypass vulnerability in Microsoft Windows SmartScreen	Yes	Yes	Yes	False
CVE-2024-40890	Zyxel	DSL CPE Devices	An OS Command Injection Vulnerability in the Zyxel DSL CPE series	Yes	No	Yes	False
CVE-2024-40891	Zyxel	DSL CPE Devices	An OS Command Injection Vulnerability in the Zyxel DSL CPE series	Yes	Yes	Yes	False
CVE-2024-41710	Mitel	SIP Phones	A Command Injection Vulnerability in Mitel 6800, 6900, and 6900w series SIP phones, including the 6970 Conference Unit, could allow attackers to execute arbitrary commands	No	Yes	Yes	False

			within the phone's context				
CVE-2024-45195	Apache	OFBiz	A Forced Browsing Vulnerability in the Apache OFBiz enables remote attacker to gain unauthorized access	No	No	Yes	False
CVE-2024-47945	ThinkPHP	ThinkPHP	A Local File Inclusion (LFI) Vulnerability in ThinkPHP allows an unauthenticated remote attacker to execute arbitrary operating system commands	No	No	No	False
CVE-2024-49035	Microsoft	Partner Center	An Improper Privilege Management Vulnerability in Partner.Microsoft.com	No	No	Yes	False
CVE-2024-53104	Linux	Kernel	An Out-of-Bounds Write Vulnerability in UVCVideo Driver in Linux Kernel leads to potential memory corruption	Yes	No	Yes	True
CVE-2024-57727	SimpleHelp	SimpleHelp	An Unauthenticated Path Traversal Vulnerability in the SimpleHelp Remote Monitoring and Management (RMM)	No	Yes	Yes	False

			software allows unauthenticated attackers to download arbitrary files from the server				
CVE-2024-57968	Advantive	VeraCore	An Upload Validation Vulnerability in Advantive VeraCore allows remote authenticated users to upload files to unauthorized folders	Yes	Yes	No	False
CVE-2023-34192	Synacor	Zimbra Collaboration Suite (ZCS)	A Cross-Site Scripting (XSS) Vulnerability in Synacor Zimbra Collaboration Suite (ZCS)	No	No	Yes	False
CVE-2023-49103	ownCloud	owncloud/ graphapi	A Sensitive Information Disclosure Vulnerability in the ownCloud owncloud/graphapi	No	No	Yes	False
CVE-2022-23748	Audinate	Dante Discovery	A Process Control Vulnerability in the Dante Discovery's mDNSResponder.exe enables DLL sideloading	No	Yes	Yes	False
CVE-2020-15069	Sophos	XG Firewall	A Buffer Overflow Vulnerability in Sophos XG Firewall could allow remote code execution	No	Yes	Yes	False
CVE-2020-29574	Sophos	Cyberpam OS	An SQL Injection	No	Yes	Yes	False

			Vulnerability in the WebAdmin interface of CyberoamOS(CROS), enabling an unauthenticated attacker to remotely execute arbitrary SQL statements				
CVE-2018-9276	Paessler	PRTG Network Monitor	An OS Command Injection Vulnerability in Paessler PRTG Network Monitor	No	No	Yes	False
CVE-2018-19410	Paessler	PRTG Network Monitor	A Local File Inclusion Vulnerability in the Paessler PRTG Network Monitor	No	No	Yes	False
CVE-2017-3066	Adobe	ColdFusion	A Deserialization Vulnerability in the Apache BlazeDS library affects Adobe ColdFusion	No	Yes	Yes	False

Ransomware Insights for January

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

Ransomware	Description	No.of Affected Organizations for February-2025	Targeted Industries	Vulnerabilities Abused Most
Clop	Clop ransomware is a sophisticated cyber threat first identified in 2019, known for its double-extortion tactics and	335	• Healthcare • Bank • Education • Gaming	• CVE-2024-55956 • CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351

	targeted attacks on large organizations. Operated by the financially motivated cybercrime group TA505, Clop not only encrypts victim data but also exfiltrates sensitive information, threatening public disclosure unless a ransom is paid. The ransomware has been linked to high-profile attacks exploiting vulnerabilities in widely used software, including the MOVEit Transfer and Accellion File Transfer Appliance (FTA). Clop operators gain initial access through phishing campaigns, exploiting zero-day vulnerabilities, or leveraging compromised credentials.		• Transportation	• CVE-2023-34362 • CVE-2023-47246
Ransomhub	Ransomhub is a self-described Ransomware-as-a-Service operation first disclosed in announcements on the Russian-language dark web forum RAMP in February 2024. The encryptor has versions written in C++ and the Go programming language and claims to support encryption of Windows, Linux, and ESXi devices. Initial posts announcing the group explicitly forbid attacks on the Commonwealth of Independent States, Cuba, North Korea, and China, as well as encryption of non-profit hospitals. At the time of this report, Ransomhub has publicly claimed five distinct organizations across nine posts from February 10th to March 4th on its data leak site	95	• Education • Construction • Government	CVE-2020-1472
Akira	Akira ransomware underscored a critical security vulnerability linked to the lack of Multi-Factor Authentication (MFA). The nations experiencing the fallout encompass the United States, the United Kingdom, Canada, Australia, and South Korea. The repercussions are noteworthy,	80	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259

	especially within pivotal domains like Services and Goods, Manufacturing, Education, and Finance.			
FOG	Fog ransomware, emerging in May 2024, initially targeted educational and recreational sectors by exploiting compromised VPN credentials to infiltrate systems. More recently, the group has shifted focus toward high-revenue sectors like financial services, broadening its victim base and refining tactics to maximize ransom potential. This adaptive approach underscores Fog ransomware's escalating threat, as it increasingly prioritizes industries where operational disruption could drive substantial ransom demands.	52	• Education • Recreation	• CVE-2024-40711 • CVE-2024-40766
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.	38	• Education • Healthcare	• Unknown
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	32	• Healthcare • Finance • Technology • Manufacturing	• CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-34362 • CVE-2023-47246 • CVE-2022-2295

	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.			
Play	The Play ransomware group, also identified as Balloonfly and PlayCrypt, has significantly impacted businesses and critical infrastructure across North America, South America and Europe regions. With a primary focus on telecommunications, the group has extended its reach to healthcare, technology and media industries. It was observed that the group focused on managed service providers (MSPs) globally, using remote monitoring and management (RMM) tools to infiltrate customer systems. Their campaigns involve custom tools like "Grixba" and "VSS Copying Tool" written in .NET. Interestingly, Play ransomware affiliates prefer email communication for negotiations and do not provide Tor negotiation page links in ransom notes on compromised systems.	30	• Healthcare • Media • Technology • Telecommunication	• CVE-2022-41040 • CVE-2022-41080 • CVE-2022-41082 • CVE-2021-34523 • CVE-2020-12812 • CVE-2018-13379
Lynx	Lynx ransomware, active since mid-2024, is a sophisticated malware operating under a ransomware-as-a-service (RaaS) model, claiming over 20 victims across various industries. It employs single and double extortion tactics, encrypting critical files with a ".lynx" extension and threatening to leak data if ransoms are unpaid, while also deleting backups like shadow copies to hinder recovery. Notably, Lynx has targeted organizations in the United States, United Kingdom,	30	• Finance • Retail • Real Estate • Manufacture • Construction • Logistic	• Unknown

	Canada, Guatemala, and Australia, with a significant attack on Romania's Electrica Group, demonstrating its capacity to disrupt critical infrastructure. The ransomware employs a hybrid encryption method, using AES for file encryption and RSA for key protection, and directs victims to Tor communication channels for ransom negotiations. Key features include targeting specific directories for encryption, terminating processes, encrypting network drives, escalating privileges, and altering system settings, such as background images. By employing these sophisticated techniques, Lynx continues to pose a serious threat to industries worldwide.			
Funksec	Funksec is a recently identified extortion group that has claimed 11 victims across sectors such as media, IT, education, and critical infrastructure, including healthcare, financial services, and government entities. Operating a Tor-based data leak site (DLS) created between late November and early December 2024, Funksec centralizes its ransomware activities and advertises a free DDoS tool, with indications that it may develop its own ransomware binary, showcasing its technical sophistication. The group's first known advertisement, titled "Funksec Ransomware," was posted on December 3, 2024. Funksec has targeted regions with advanced digital infrastructure, including the United States, Europe, and parts of Asia, where higher financial rewards are anticipated due to the critical nature of operations. Linked to sophisticated threat	18	• Healthcare • Finance • Government • Information technology • Education	• Unknown

	actors from Russia, China, Iran, North Korea, and other independent cybercriminal groups, Funksec leverages ransomware-as-a-service (RaaS) models and software vulnerabilities to expand its impact. Despite its capabilities, limited information is currently available regarding its tactics, techniques, and procedures (TTPs), and no direct association with other known threat groups has been identified.			
Bianlian	BianLian is a Golang-based ransomware that significantly threatens diverse industries, including healthcare, education and government entities. Recognizing the severity of this threat, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and Australian Cyber Security Centre (ACSC) have collaboratively issued advisories, emphasizing the group's focus on critical infrastructure sectors in the United States and Australia. Upon infiltrating systems, the 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.	17	• Healthcare • Banking • Utilities • Insurance	• CVE-2023-27350 • CVE-2022-27925 • CVE-2022-37042 • CVE-2021-4034 • CVE-2021-31207 • CVE-2021-34473 • CVE-2021-34523
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	9	• Healthcare • Education • Research	• Unknown

	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.			

Conclusion

The significant increase in CISA KEV additions in February 2025 highlights a clear escalation in adversaries actively exploiting both newly disclosed and previously known vulnerabilities. To mitigate these evolving threats, organizations must prioritize prompt remediation of KEV-listed vulnerabilities while enhancing detection, response, and monitoring capabilities to address zero-day exploitation and malware leveraging these weaknesses. Loginsoft Vulnerability Intelligence (LOVI) delivers critical, real-time insights to help organizations stay ahead of emerging threats, strengthen their defenses, and proactively safeguard their critical assets against future attacks.

Reference Links:

- https://www.cisa.gov/news-events/alerts/2025/02/13/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/02/12/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2023/11/30/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/02/04/cisa-adds-four-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/02/05/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/02/06/cisa-adds-five-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/02/11/cisa-adds-four-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/02/07/cisa-adds-one-known-exploited-vulnerability-catalog
- https://news.sophos.com/ja-jp/2024/10/31/pacific-rim-timeline-jp/
- https://research.checkpoint.com/2023/stayin-alive-targeted-attacks-against-telecoms-and-government-ministries-in-asia/
- https://cert.gov.ua/article/6282536

- https://fieldeffect.com/blog/field-effect-mitigates-not-so-simplehelp-exploits-enabling-deployment-of-backdoors
- https://intezer.com/blog/research/xe-group-exploiting-zero-days/
- https://www.akamai.com/blog/security-research/2025-january-new-aquabot-mirai-variant-exploiting-mitel-phones
- https://www.greynoise.io/blog/active-exploitation-of-zero-day-zyxel-cpe-vulnerability-cve-2024-40891
- https://cyble.com/threat-actor-profiles/sofacy/
- https://wpsites.ucalgary.ca/jacobson-cpsc/2025/01/25/us-treasury-hacked-by-chinese-sponsored-hackers/
- https://www.trendmicro.com/en_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html