loginsoft

Monthly Report

Threat & Vulnerabilities Report – November 2025

Summary

November saw a pronounced shift in adversary activity, with attackers increasingly targeting both critical infrastructure and broadly deployed software assets. A total of 11 vulnerabilities were added to the CISA Known Exploited Vulnerabilities (KEV) catalog, affecting a diverse range of vendors including Fortinet, Gladinet, Microsoft, WatchGuard, Samsung, CWP, Google, Oracle, and OpenPLC, underscoring persistent exploitation across enterprise, cloud, and application-layer technologies.

Beyond the catalogued CVEs, active attacks were also reported against outdated ASUS routers, the Noo JobMonster WordPress theme, the Sneeit Framework plugin, and 7-Zip, despite the latter having previously released patches.

Ransomware operations continued to escalate, with Qilin, Clop, and Akira leading significant attack activity across the threat landscape. Key sectors such as healthcare, education, and manufacturing remained primary targets, with adversaries weaponizing both existing and emerging vulnerabilities to gain initial access, execute encryption, exfiltrate sensitive data, and disrupt operational continuity.

Actively Exploited Vulnerabilities

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	CISA KEV	OSS
CVE-2025-2492	Asus	Routers	An Improper Authentication Vulnerability in the ASUS AiCloud that can be triggered by a crafted request, potentially leading to unauthorized execution of functions.	No	Yes	No	False
CVE-2025-5397	Noo	JobMonster (WordPress Theme)	An Authentication Bypass Vulnerability in the JobMonster WordPress theme that makes it possible for unauthenticated attackers to bypass standard authentication and access administrative accounts.	No	No	No	False
CVE-2025-6389	Sneeit	Sneeit Framework	An Unauthenticated Remote Code Execution Vulnerability in the Sneeit Framework plugin for WordPress that makes it possible for unauthenticated attackers to execute code on the server.	No	No	No	False
CVE-2025-9242	WatchGuard	Firebox	An Out-of-Bounds Write Vulnerability in the WatchGuard Firebox that	No	No	Yes	False

			may allow a remote unauthenticated attacker to execute arbitrary code.				
CVE-2025-9491	Microsoft	Windows	A Remote Code Execution Vulnerability in the Microsoft Windows LNK File UI Misrepresentation.	Yes	Yes	No	False
CVE-2025-11001	7-Zip	7-Zip	A File Parsing Directory Traversal Remote Code Execution Vulnerability in 7-ZIP	No	No	No	False
CVE-2025-11371	Gladinet	CentreStack and Triofox	A Local File Inclusion Vulnerability in the Gladinet CentreStack and TrioFox, that enables unintended disclosure of system files.	Yes	No	Yes	False
CVE-2025-11833	WordPress plugin developer	Post SMTP WordPress Plugin	A Missing Authorization Vulnerability in the Post SMTP WordPress Plugin that enables complete takeover of the affected account.	No	No	No	False
CVE-2025-12480	Gladinet	Triofox	An Improper Access Control Vulnerability in the Gladinet Triofox that enables an attacker to bypass authentication and access the configuration pages, resulting in the upload and execution of arbitrary payloads.	No	Yes	Yes	False
CVE-2025-13223	Google	Chromium V8	A Type Confusion Vulnerability in the Google Chromium V8 that allows for heap corruption.	Yes	No	Yes	False
CVE-2025-21042	Samsung	Mobile Devices	An Out-of-Bounds Write Vulnerability in the Samsung mobile devices in the libimagecodec.quram.so.	Yes	Yes	Yes	False
CVE-2025-48703	CWP	Control Web Panel	An OS Command Injection Vulnerability in the Control Web Panel that allows unauthenticated remote code execution via shell metacharacters in ***t_total*** parameter in a ***filemanager changePerm*** request.	No	No	Yes	False
CVE-2025-58034	Fortinet	FortiWeb	An OS Command Injection Vulnerability in the Fortinet FortiWeb that allows authenticated attacker to execute unauthorized code on the underlying system via crafted HTTP requests	Yes	No	Yes	False
CVE-2025-61757	Oracle	Fusion Middleware	A Missing Authentication for Critical Function	Yes	No	Yes	False

			Vulnerability in the Oracle Fusion Middleware that allows unauthenticated remote attackers to take over Identity Manager.				
CVE-2025-62215	Microsoft	Windows	A Race Condition Vulnerability in Microsoft Windows that enables a local attacker with low-level privileges to escalate privileges.	Yes	No	Yes	False
CVE-2025-64446	Fortinet	FortiWeb	A Path Traversal Vulnerability in the Fortinet FortiWeb that allows an unauthenticated attacker to execute administrative commands on the system.	Yes	No	Yes	False
CVE-2021-26829	OpenPLC	ScadaBR	A Cross-Site Scripting Vulnerability in the OpenPLC ScadaBR via system_settings.shtm.	No	Yes	Yes	False

Ransomware Insights for November 2025

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 November	Targeted Industries	Vulnerabilities Abused Most
Qilin	The Qilin ransomware has been in existence since August 2022, also recognized as Agenda, and has posed a substantial threat. Employing Rust and Go programming languages, this ransomware group executes intricate and elusive attack strategies. It's developed in Rust and identified as Ransom.Win32.AGENDA.THIAFBB, was discovered. Remarkably, this ransomware initially scripted in Go language was notorious for its focus on healthcare and education sectors, particularly in nations such as Thailand and Indonesia.	101	Education Healthcare	CVE-2025-31324 CVE-2024-21762 CVE-2024-55591 CVE-2023-27532
Clop	Clop ransomware is a sophisticated cyber threat first identified in 2019, known for its double-extortion tactics and 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	98	Healthcare Bank Education Gaming Transportation	CVE-2024-55956 CVE-2023-0669 CVE-2023-27350 CVE-2023-27351 CVE-2023-34362 CVE-2023-47246

	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.			
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, especially within pivotal domains like Services and Goods, Manufacturing, Education, and Finance.	87	Education Manufacture Finance	CVE-2020-1472 CVE-2020-3259
Inc Ransom	Inc. ransomware, which emerged in June 2023, spread through spear-phishing emails and targeted vulnerable services, such as the exploitation of **CVE-2023-3519** in Citrix NetScaler. Our observations indicate that Inc. ransomware has deliberately targeted a range of sectors, including healthcare, education, and government entities. This ransomware operates as a multi-extortion scheme, involving the theft of victim data and threats to release the data online unless the victim complies with their demands.	51	Education Healthcare Government sectors	CVE-2023-3519
Sinobi	Sinobi ransomware is a sophisticated threat, suspected to be a rebrand of the Lynx ransomware group, employing double-extortion tactics that exfiltrate sensitive data before encrypting systems using Curve-25519 and AES-128-CTR algorithms. It has targeted a wide range of industries, including healthcare, manufacturing, legal services, education, and construction/engineering, highlighting its broad attack strategy. To mitigate risk, organizations are advised to implement multi-factor authentication, secure VPN access, keep systems updated with patches, train employees on phishing and safe practices, maintain offline backups, and monitor network activity for unusual behavior.	21	Healthcare Manufacturing Legal Services Education Construction	Unknown
Safepay	SafePay is a newly emerging ransomware strain believed to be derived from leaked LockBit source code, distinguished by its	14	Education Finance Agriculture	Unknown

	ransom note titled "readme_safepay.txt" and encrypted file extensions labeled ".safepay." While bearing similarities to LockBit, SafePay's refined approach establishes it as a formidable new player in the ransomware landscape. It employs a two-phase attack strategy involving initial system infiltration followed by data encryption, often using anti-detection mechanisms to evade security measures. Linked to the LockBit ransomware builder, SafePay is suspected to involve experienced cybercriminals in its creation and deployment. The ransomware primarily targets payment processors and banks, posing a significant threat to financial institutions. With at least 22 victims reported so far, SafePay's sophisticated techniques for spreading and exfiltrating data underscore its potency and highlight the challenges of mitigating its impact.		Manufacturing Healthcare Logistic	
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.	14	Healthcare Media Technology Telecommunication	CVE-2022-41040 CVE-2022-41080 CVE-2022-41082 CVE-2021-34523 CVE-2020-12812 CVE-2018-13379
Rhysida	Rhysida ransomware has a new variant that provides Ransomware-as-a-service (RaaS). As of 2023, approximately 50 victims have been identified, targeting the Education, Healthcare, Manufacturing, Information Technology and Government sectors. The deployment of Rhysida involves various methods, including the use of Cobalt Strike or a similar framework, as well as phishing campaigns. Notably, we have observed the threat actor exploiting Zerologon's (CVE-2020-1472) vulnerability, a critical elevation	11	Education Healthcare Manufacturing Information Technology Government sectors	CVE-2020-1472

	of privileges flaw in Microsoft's Netlogon Remote Protocol. Upon gaining network access, the Rhysida gang employs Living off the Land Binaries (LoLBins) techniques to execute malicious activities discreetly and avoid detection.			
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.	11	Healthcare Finance Technology Manufacturing	CVE-2023-0669 CVE-2023-27350 CVE-2023-27351 CVE-2023-34362 CVE-2023-47246 CVE-2022-2295
Handala	Handala is a politically motivated ransomware group active since late 2023, primarily targeting Israeli organizations across critical sectors such as energy, healthcare, government, education, and defense, with spillover attacks affecting U.S. infrastructure and other countries including Canada, Germany, and Australia. Known for blending ransomware with wiper tactics and data leaks, the group uses politically charged messaging to justify its campaigns, often tied to the Israel-Palestine conflict. High-profile incidents include breaches of Israeli energy firms, hospitals, academic institutions, and defense-linked companies, with stolen data volumes reaching terabytes and ransom demands up to 8 BTC. Handala's operations reflect a mix of ideological hacktivism and disruptive intent, positioning it as a serious threat to critical infrastructure globally.	6	Healthcare Energy Manufacturing Government sector Education Defense	Unknown
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	2	Finance Retail Real Estate Manufacture Construction Logistic	Unknown

	organizations in the United States, United Kingdom, 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.			

Conclusion

As attackers increasingly engineer their own points of entry, overlooked infrastructure and unsupported systems are becoming liability multipliers, reinforcing the urgency for proactive visibility and threat-driven prioritization. The combined rise in ransomware targeting critical sectors and abuse of already known vulnerabilities reflects a shift toward persistence-driven operations rather than opportunistic attacks. In such an environment, situational awareness outweighs patch availability. Platforms like Loginsoft Vulnerability Intelligence (LOVI) empower security teams with real-time exploit insights, threat actor tracking, and actionable intelligence, enabling faster detection and response in an ever-evolving threat landscape.