loginsoft

Monthly Report

Threat & Vulnerabilities Report – December 2025

Summary

December closed out 2025 by exposing a hardened exploitation environment, where high-impact vulnerabilities were rapidly absorbed into active attack chains. During the month, 20 vulnerabilities were added to the CISA Known Exploited Vulnerabilities (KEV) catalog, spanning major vendors such as Microsoft, Google, Apple, Fortinet, and ASUS. The breadth of affected products highlighted sustained adversarial focus across both consumer and enterprise platforms that underpin global digital infrastructure.

A key standout was a Meta React Server Components vulnerability, which was actively exploited by multiple threat actors and assessed to pose a long-term risk due to its widespread adoption and deep integration within modern web applications.

Ransomware activity remained elevated, with Qilin, Akira, and Safepay driving a significant share of high-impact intrusions across the threat landscape. Adversaries continued to target critical sectors such as healthcare, education, and manufacturing, chaining both newly disclosed and long-standing vulnerabilities to obtain initial access, deploy encryption payloads, exfiltrate sensitive data, and cause widespread operational disruption.

Actively Exploited Vulnerabilities

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	CISA KEV	OSS
CVE-2025-6218	RARLAB	WinRAR	A Path Traversal vulnerability in RARLAB WinRAR allows an attacker to execute code in the context of the current user.	No	Yes	Yes	False
CVE-2025-8110	Gogs	Gogs Self-Hosted Git Service	An Improper Symbolic link handling vulnerability in Gogs Git service enables remote code execution	Yes	No	No	True
CVE-2025-8489	WordPress plugin ecosystem	King Addons for Elementor – Free Elements, Widgets, Templates, and Features for Elementor plugin for WordPress	A Privilege Escalation vulnerability in the King Addons for Elementor - Free Elements, Templates, and Features for Elementor plugin for WordPress that makes it possible for unauthenticated attackers to register with administrator-level user accounts.	No	No	No	False
CVE-2025-14174	Google	Chromium	An Out of Bounds Memory Access vulnerability in the Google Chromium that could allow a remote	Yes	No	Yes	False

			attacker to perform out of bounds memory access via a crafted HTML page.				
CVE-2025-14611	Gladinet	CentreStack and Triofox	A Hard Coded Cryptographic vulnerability in Gladinet CentreStack and Triofox	No	No	Yes	False
CVE-2025-14733	WatchGuard	Firebox	An Out of Bounds Write vulnerability in the WatchGuard Firebox in the OS iked process.	Yes	No	Yes	False
CVE-2025-14847	MongoDB	MongoDB and MongoDB Server	An Improper Handling of Length Parameter Inconsistency vulnerability in MongoDB and MongoDB Server	No	No	Yes	False
CVE-2025-20393	Cisco	Multiple Products	An Improper Input Validation vulnerability in Cisco Multiple Products that allows threat actors to execute arbitrary commands with root privileges on the underlying operating system of an affected appliance.	Yes	Yes	Yes	False
CVE-2025-40602	SonicWall	SMA1000 appliance	A Missing Authorization vulnerability in SonicWall SMA1000 that could allow for privilege escalation	Yes	No	Yes	False
CVE-2025-43529	Apple	Multiple Products	A Use-After-Free WebKit vulnerability in Apple Multiple products that can lead to memory corruption.	Yes	No	Yes	False
CVE-2025-48572	Android	Framework	A Privilege Escalation vulnerability in the Android Framework	No	No	Yes	True
CVE-2025-48633	Android	Framework	An Information Disclosure vulnerability in the Android Framework	No	No	Yes	True
CVE-2025-55182	Meta	React Server Components	A Remote Code Execution vulnerability Meta React Server Components that allows an unauthenticated remote code execution by exploiting a flaw in how React decodes payloads sent to React Server Function endpoints.	No	Yes	Yes	False

CVE-2025-58360	OSGeo	GeoServer	An Improper Restriction of XML External Entity Reference vulnerability in the OSGeo GeoServer	No	No	Yes	True
CVE-2025-59374	ASUS	Live Update	An Embedded Malicious Code vulnerability in the ASUS Live Update	No	Yes	Yes	False
CVE-2025-59718	Fortinet	• FortiOS • FortiSwitchMaster • FortiProxy • FortiWeb	An Improper Verification of Cryptographic Signature vulnerability in Fortinet multiple products that may allow an unauthenticated attacker to bypass the FortiCloud SSO login authentication via a crafted SAML message.	No	No	Yes	False
CVE-2025-62221	Microsoft	Windows	A Use After Free vulnerability in Microsoft Windows that allows an authorized attacker to elevate privileges locally.	Yes	No	Yes	False
CVE-2025-66644	Array Networks	ArrayOS AG	An OS Command Injection vulnerability in the Array Networks ArrayOS AG that allows an attacker to execute arbitrary commands.	No	No	Yes	False
CVE-2023-52163	Digiever	DS-2105 Pro	A Missing Authorization vulnerability in Digiever DS-2105 Pro allows for command injection via ***time_tzsetup.cgi***.	No	Yes	Yes	False
CVE-2022-37055	D-Link	Routers	A Buffer Overflow vulnerability in the D-Link Routers that has high impact on confidentiality, integrity and availability.	No	Yes	Yes	False
CVE-2021-26828	OpenPLC	ScadaBR	An Unrestricted Upload of File with Dangerous Type vulnerability in the OpenPLC ScadaBR that allows remote authenticated users to upload and execute arbitrary JSP files via ***view_edit.shtm***.	No	Yes	Yes	False
CVE-2018-4063	Sierra Wireless	AirLink ALEOS	An Unrestricted Upload of File with Dangerous Type vulnerability in Sierra Wireless AirLink ALEOS allows an attacker to craft an authenticated HTTP request that uploads	No	No	Yes	False

			malicious files and triggers arbitrary code execution on the device.				

Ransomware Insights for December 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 December 2025	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.	166	• Education • Healthcare	• CVE-2025-31324 • CVE-2024-21762 • CVE-2024-55591 • CVE-2023-27532
Lockbit5	LockBit 5 represents the continued evolution of the LockBit ransomware lineage, emphasizing speed, automation, and operational resilience. The variant refines fast encryption routines, aggressive data exfiltration, and highly automated deployment to minimize attacker dwell time while maximizing impact. LockBit 5 maintains a mature ransomware-as-a-service (RaaS) ecosystem, complete with affiliate tooling, leak portals, and negotiation infrastructure. Technically, it shows improved evasion techniques, flexible payload customization, and streamlined lateral movement to accelerate network-wide compromise.	86	• Technology • Manufacturing • Healthcare	Unknown
	Akira ransomware underscored a critical security vulnerability linked			

Akira	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	71	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259
Safepay	SafePay is a newly emerging ransomware strain believed to be derived from leaked LockBit source code, distinguished by its ransom note titled "readme_safepay.txt" and encrypted file extensions labeled ".safepay." While bearing similarities to LockBit, SafePay's refined approach establishes it as a formidable new player in the ransomware landscape. It employs a two-phase attack strategy involving initial system infiltration followed by data encryption, often using anti-detection mechanisms to evade security measures. Linked to the LockBit ransomware builder, SafePay is suspected to involve experienced cybercriminals in its creation and deployment. The ransomware primarily targets payment processors and banks, posing a significant threat to financial institutions. With at least 22 victims reported so far, SafePay's sophisticated techniques for spreading and exfiltrating data underscore its potency and highlight the challenges of mitigating its impact.	67	• Education • Finance • Agriculture • Manufacturing • Healthcare • Logistic	Unknown
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,	54	• Healthcare • Manufacturing • Legal Services • Education • Construction	Unknown

	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.			
Devman	DevMan ransomware is characterized by its opportunistic yet technically efficient attack model, often targeting exposed services and misconfigured systems for rapid intrusion. The malware emphasizes fast execution, combining credential harvesting and lightweight lateral movement before deploying its encryption payload. DevMan typically incorporates data exfiltration to support double-extortion tactics, increasing pressure during ransom negotiations. Its tooling is streamlined to reduce operational noise while maintaining persistence and control over compromised environments.	46	• Technology • Healthcare • Public Sector	Unknown
Dragonforce	DragonForce is a ransomware group originating from Malaysia. Initially, known as a hacktivist group, DragonForce has transitioned into a ransomware operation, threatening victims with data encryption and extortion demands. They have targeted various industries and organizations globally, including government entities, businesses, and critical infrastructure sectors. The group gained attention for their attacks on American companies, with details about data compromise and motives undisclosed. DragonForce has also threatened to release stolen information on dark web leak sites to pressure victims into paying ransoms.	35	• Government entities • Infrastructure sectors	• CVE-2024-57726 • CVE-2024-57727 • CVE-2024-57728 • CVE-2022-26134
	Inc. ransomware, which emerged in June 2023, spread through spear-phishing emails and targeted vulnerable services, such as the		• Education	

IncRansom	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.	29	• Healthcare • Government sectors	• CVE-2023-3519
Coinbasecartel	Coinbase Cartel ransomware distinguishes itself through its strong emphasis on data theft and psychological pressure rather than purely large-scale encryption. The operation typically prioritizes exfiltration of sensitive data early in the intrusion, using it as primary leverage while selectively encrypting systems to amplify impact. Its tooling is relatively lightweight but focused on stealth, often minimizing noisy lateral movement to evade detection during prolonged dwell time. The group is also notable for aggressive negotiation tactics and curated victim shaming strategies, using tailored leak threats to maximize coercion rather than relying solely on automated extortion workflows.	22	• Technology • Logistics • Financial Services	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 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	13	• Finance • Retail • Real Estate • Manufacture • Construction • Logistic	Unknown

	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

Collectively, December's activity underscored how rapidly attackers operationalized both vulnerabilities and ransomware, with groups such as Qilin, Akira, and Safepay dominating high-impact intrusions through mature, well-orchestrated campaigns. The convergence of fast weaponization and scalable ransomware operations reinforced the need for accelerated patching, continuous exposure monitoring, and sharper risk prioritization. **Loginsoft Vulnerability Intelligence (LOVI)** brings this clarity by correlating real-world exploitation with active threat trends, enabling teams to focus defenses where risk is actively materializing rather than where it merely exists.