loginsoft

Monthly Report

Threat & Vulnerabilities Report – January 2026

Executive Summary

2026 opened with a sharp escalation in real-world exploitation, underscoring how quickly both newly disclosed and long-standing vulnerabilities can be operationalized by threat actors. Over the month, 17 vulnerabilities were added to the CISA Known Exploited Vulnerabilities (KEV) catalog, including three affecting Microsoft products, two tied to SmarterTools, and critical issues spanning vendors such as Ivanti, Fortinet, Linux, GNU InetUtils, Broadcom, Synacor, Versa, Vite, Cisco, Prettier, Gogs, and Hewlett Packard.

Beyond KEV additions, active exploitation was observed across multiple enterprise, infrastructure, and open-source platforms, highlighting sustained attacker focus on management planes, developer ecosystems, and network edge technologies.

Ransomware activity intensified throughout the month, led by Qilin with 108 impacted organizations, followed by Akira affecting 58 entities, and Sinobi with 56 confirmed victims, collectively driving a sharp rise in high-impact intrusions across critical sectors. Threat actors continued to focus on critical sectors including healthcare, education, and manufacturing, leveraging a mix of newly disclosed and long-standing vulnerabilities to gain initial access, deploy encryption payloads, exfiltrate sensitive data, and amplify operational disruption.

Vulnerabilities added to the CISA KEV catalog in January 2026

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-1281	Ivanti	Endpoint Manager Mobile (EPMM)	A Code Injection vulnerability in Ivanti Endpoint Manager Mobile (EPMM) that allows attackers to achieve unauthenticated remote code execution.	Yes	No	False
CVE-2026-20045	Cisco	Unified Communications Manager	A Code Injection vulnerability in Cisco Unified Communications Products that enables an attacker to obtain user-level access to the underlying operating system and then elevate privileges to root.	Yes	No	False
CVE-2026-20805	Microsoft	Windows	An Information Disclosure vulnerability in Microsoft Windows that enables an authorized attacker to disclose information locally.	Yes	No	False
CVE-2026-21509	Microsoft	Office	A Security Feature Bypass vulnerability in Microsoft Office that could allow an unauthorized attacker to bypass a security feature locally.	Yes	No	False
CVE-2026-23760	SmarterTools	SmarterMail	An Authentication Bypass Using an Alternate Path or Channel vulnerability in SmarterTools SmarterMail that can lead to full administrative compromise of the SmartMail instance.	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-24061	GNU	InetUtils	An Argument Injection vulnerability in GNU InetUtils that could enable remote authentication bypass via a "***-f root***" value for the USER environment variable.	No	No	False
CVE-2026-24858	Fortinet	Multiple Products	An Authentication Bypass Using an Alternate Path or Channel vulnerability in Fortinet multiple products allows an attacker with a FortiCloud account and a registered device to log into other devices registered to other accounts, if FortiCloud SSO authentication is enabled on those devices.	Yes	No	False
CVE-2025-8110	Gogs	Gogs	A Path Traversal vulnerability in Gogs PutContents API that could allow for code execution.	Yes	No	True
CVE-2025-31125	Vite	Vitejs	An Improper Access Control vulnerability in Vite Vitejs that exposes content of non-allowed files using ***?inline&import*** or ***?raw?import***.	No	No	False
CVE-2025-34026	Versa	Concerto	An Improper Authentication vulnerability in Versa Concerto in Traefik reverse proxy configuration, that allows an attacker to access administrative endpoints.	Yes	No	False
CVE-2025-37164	Hewlett Packard Enterprise (HPE)	OneView	A Code Injection vulnerability in Hewlett Packard Enterprise (HPE) OneView that enables a remote unauthenticated user to perform remote code execution.	No	Yes	False
CVE-2025-52691	SmarterTools	SmarterMail	An Unrestricted Upload of File with Dangerous Type vulnerability in SmarterTools SmarterMail that allows an unauthenticated attacker to upload arbitrary files to any location on the mail server enabling remote code execution.	No	No	False
CVE-2025-54313	Prettier	eslint-config-prettier	An Embedded Malicious Code vulnerability in the Prettier eslint-config-prettier	No	Yes	True

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2025-68645	Synacor	Zimbra Collaboration Suite (ZCS)	A PHP Remote File Inclusion vulnerability in Synacor Zimbra Collaboration Suite (ZCS) allows remote attackers to craft requests to the /h/rest endpoint.	No	No	False
CVE-2024-37079	Broadcom	VMware vCenter Server	An Out-of-Bounds Write vulnerability in Broadcom VMware vCenter in the implementation of the DCERPC protocol.	No	No	False
CVE-2018-14634	Linux	Kernal	An Integer Overflow vulnerability in Linux Kernel that allows an unprivileged local user with access to SUID binary to escalate privileges on the system.	No	No	False
CVE-2009-0556	Microsoft	Office	A Code Injection vulnerability in Microsoft Office PowerPoint that allows remote attackers to execute arbitrary code via PowerPoint file with an ***OutlineTextRefAtom*** containing an invalid index value that triggers memory corruption.	No	No	False

Actively Exploited Vulnerabilities in January 2026

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-0625	D-Link	• DSL-526B • DSL-2640B • DSL-2740R • DSL-2780B	A Command Injection vulnerability in the D-Link DSL gateway devices in the ***dnscfg.cgi*** endpoint.	Yes	Yes	False
CVE-2026-0920	LA-Studio	LA-Studio Element Kit for Elementor	An Authentication Bypass vulnerability in the LA-Studio Element Kit for Elementor plugin for WordPress that enables unauthenticated attackers to create administrator accounts.	No	No	False
CVE-2026-1340	Ivanti	Endpoint Manager Mobile (EPMM)	A Code Injection vulnerability in Ivanti Endpoint Manager Mobile (EPMM) that allows attackers to achieve	Yes	No	False

			unauthenticated remote code execution.			
CVE-2026-23550	Modular DS	Modular DS	An Unauthenticated Privilege Escalation vulnerability in the Modular DS WordPress plugin	No	No	False
CVE-2025-8088	RARLAB	WinRAR	A Path Traversal vulnerability in RARLAB WinRAR that could enable an attacker to execute arbitrary code by crafting malicious archive files.	No	Yes	False
CVE-2025-15521	Kodezen	Academy_lms	An Unauthenticated Privilege Escalation vulnerability in the Academy LMS WordPress LMS Plugin for Complete eLearning Solution enables unauthenticated attackers to takeover administrative accounts.	No	No	False
CVE-2025-53690	Sitecore	Multiple Products	A Deserialization of Untrusted Data vulnerability in Sitecore multiple products that enables an attacker to exploit exposed ASP.NET machine keys to achieve remote code execution.	No	Yes	False
CVE-2025-64155	Fortinet	FortiSIEM	An OS Command Injection vulnerability in Fortinet FortiSIEM that allows an unauthenticated attacker to execute arbitrary commands via specially crafted TCP requests.	No	No	False
CVE-2020-16040	Google	Chrome	An Insufficient Data Validation vulnerability in V8 in Google Chrome allows a remote attacker to potentially exploit heap corruption via a crafted HTML page.	No	Yes	False

Ransomware Insights for January 2026

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 in January 2026	Targeted Industries	Vulnerabilities abused most
Qilin	Qilin Ransomware is characterized by a highly structured and professionalized ransomware-as-a-service(RaaS) model, supported by technically mature and repeatable attack workflows. Initial access is commonly achieved through compromised credentials, exposed services, or the abuse of known weaknesses, after which a modular payload is deployed to encrypt data and disrupt business operations. The ransomware incorporates multiple evasion techniques to hinder detection and analysis, while its architecture supports flexible deployment and updates. A dedicated Tor-based portal is used for victim communication and ransom negotiation, reflecting an organized extortion framework. Multiple variants have been observed over time, indicating ongoing development and adaptation of the malware family.	108	• Manufacturing • Healthcare • Technology • Business Services • Financial Services	• CVE-2025-31324 • CVE-2024-21762 • CVE-2024-55591 • CVE-2023-27532
Akira	Akira is a ransomware-as-a-service (RaaS) operation distinguished by its early and aggressive focus on virtualized infrastructure. Beyond standard double-extortion tactics, Akira rapidly introduced a Linux encryptor specifically designed for VMware ESXi, enabling attackers to halt and encrypt large numbers of virtual machines from a single hypervisor using VM-aware options like vmonly and stopvm. Post-compromise activity prioritizes identity systems, backup platforms, and hypervisors, allowing fast, high-impact disruption of entire environments. This hypervisor-centric design, combined with data exfiltration via tools like rclone and SCP, makes Akira particularly effective against modern, virtualization-heavy networks.	58	• Manufacturing • Business Services • Technology • Construction • Agriculture	• CVE-2024-37085 • CVE-2024-40711 • CVE-2024-40766 • CVE-2023-20269 • CVE-2023-20363 • CVE-2023-27532 • CVE-2023-28252 • CVE-2023-48788 • CVE-2022-40684 • CVE-2021-21972 • CVE-2020-3259 • CVE-2020-3580 • CVE-2019-6693

Ransomware	Description	No of affected organizations in January 2026	Targeted Industries	Vulnerabilities abused most
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.	56	• Healthcare • Manufacturing • Construction • Technology • Business Services	Unknown
Clop	Cl0p Ransomware originated as an evolution of the CryptoMix malware family and first emerged in early 2019, quickly establishing itself as a sophisticated and financially motivated threat. Commonly associated with the TA505/FIN11 ecosystem and tracked clusters such as UNCA2546 and UNCA2582, Cl0p operates under a ransomware-as-a-service (RaaS) model and has been used in high-impact attacks against large enterprises. Technically, Cl0p stands out for its use of digitally signed Win32 PE executables to appear legitimate and evade security controls, combined with strong encryption using RC4 for file data and RSA-1024 for key protection. Beyond encryption, Cl0p relies heavily on double-extortion tactics, threatening public data leaks if ransom demands typically paid in cryptocurrency are not met, making it both disruptive and coercive.	46	• Technology • Logistics • Manufacturing • Consumer Services • Business Services	• CVE-2023-0669 • CVE-2023-24362 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-35036 • CVE-2023-47246 • CVE-2021-27101 • CVE-2021-27102 • CVE-2021-27103 • CVE-2021-27104 • CVE-2021-35211

Ransomware	Description	No of affected organizations in January 2026	Targeted Industries	Vulnerabilities abused most
IncRansom	INC is a ransomware-as-a-service (RaaS) operation that emerged in mid-to-late 2023, operating through an affiliate-driven model in which core operators supply the malware and infrastructure while affiliates conduct intrusions and share profits. The group relies on a double-extortion strategy, coercing victims by threatening data leaks under the pretext of "protecting their reputation." INC maintains two dedicated leak sites a private, credential-protected portal used for victim communication and negotiation, and a public site used to release stolen data. First detected in July 2023 and tracked by Trend Micro as Water Anito, the ransomware encrypts files using AES algorithm, reinforcing its position as a structured and professionally run extortion operation.	44	• Healthcare • Technology • Business Services • Manufacturing • Education	• CVE-2023-3519 • CVE-2023-4966 • CVE-2023-48788
TheGentlemen	The Gentlemen Ransomware group has emerged as a steadily advancing threat actor known for its strategic targeting and disciplined operational methods. The group has focused heavily on organizations across 17 countries, with the Asia-Pacific region being most affected, particularly Thailand, followed by notable activity in the United States. Its campaigns have struck manufacturing the hardest, alongside construction, healthcare, insurance, and other critical service sectors, underscoring the group's willingness to disrupt essential infrastructure. To evade detection and maintain persistence, The Gentlemen relies on a blend of legitimate administrative tools, custom anti-AV utilities, and environment-tailored payloads, enabling stealthy lateral movement and long-term footholds.	30	• Manufacturing • Technology • Healthcare • Financial Services • Education	CVE-2025-7771
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	30	• Technology • Healthcare • Public Sector • Construction • Agriculture	Unknown

Ransomware	Description	No of affected organizations in January 2026	Targeted Industries	Vulnerabilities abused most
	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.			
Lynx	Lynx is a ransomware group that surfaced in mid-2024 and is widely assessed to be a rebrand of the INC ransomware operation, based on strong code-level overlaps between the two strains. Operating under a Ransomware-as-a-Service (RaaS) model, Lynx equips affiliates with encryption tooling, leak-site infrastructure, and operational support, allowing campaigns to scale rapidly. Rather than relying on a single intrusion vector, affiliates commonly gain access through stolen credentials often sourced from dark-web markets or infostealer logs and phishing attacks, enabling direct entry into RDP, VPN, and email environments. This combination of inherited code, flexible access methods, and an affiliate-driven ecosystem positions Lynx as a fast-moving and adaptable ransomware threat.	25	• Manufacturing • Business Services • Technology • Logistics • Agriculture	Unknown
Everest	Everest ransomware is unique for its evolution from a traditional double-extortion group into a specialized Initial Access Broker (IAB), often choosing to sell network footholds to other criminals rather than deploying encryption. A standout feature of their operation is the active recruitment of corporate insiders, offering cash payments or profit sharing in exchange for remote access via tools like RDP or AnyDesk. Their modern tactics emphasize pure data theft from external file-sharing services, achieving rapid exfiltration in mere hours to bypass the operational complexity and detection risks of traditional ransomware payloads. This hybrid model allows the group to pivot between direct extortion and the sale of access to	21	• Healthcare • Technology • Business Services • Manufacturing • Financial Services	Unknown

Ransomware	Description	No of affected organizations in January 2026	Targeted Industries	Vulnerabilities abused most
	maximize profits based on the target's profile.			
NightSpire	NightSpire, quickly positioned itself as a high-impact ransomware actor by pairing double-extortion operations with exploitation of advanced vulnerabilities. The group maintains a dark-web leak portal with countdown-based coercion and employs stealth techniques LOLBins, MEGACmd, WinSCP to exfiltrate data while remaining undetected inside victim networks. Its campaigns span the U.S., Japan, Taiwan, Egypt, and the U.K., with a notable concentration on manufacturing, reflecting a globally distributed yet technically disciplined threat posture.	19	• Manufacturing • Healthcare • Technology • Business services • Consumer services	CVE-2024-55591

Conclusion

The starting month of the year underscored a critical reality for security teams: The pattern reinforced a clear message for defenders: rapid patching, continuous exposure management, and KEV-driven prioritization remained essential as 2026 began under persistent and high-impact threat pressure. The sustained pace and scale of campaigns highlighted how both established and newly formed ransomware groups moved quickly to assert dominance in the early months of the year.