loginsoft

Monthly Report

Threat & Vulnerabilities Report – February 2026

Executive Summary

February closed with a concentrated surge in exploited vulnerabilities and ransomware activity, signaling intensified adversary focus on high-impact enterprise targets. A total of 28 vulnerabilities were added to the CISA Known Exploited Vulnerabilities (KEV) catalog, with Microsoft accounting for eight entries, followed by multiple additions impacting Cisco, Roundcube, Sangoma FreePBX, GitLab, and SolarWinds, alongside individual entries affecting Apple, Dell, and Google.

Beyond KEV updates, active exploitation activity was observed across widely deployed platforms including RARLAB WinRAR, the Linux Kernel, Atlassian Crowd, Hotta Studio products, and Microsoft Office demonstrating adversaries' continued preference for both enterprise-grade software and legacy attack surfaces.

On the ransomware front, Qilin led activity with 110 victim disclosures, followed by The Gentlemen (83) and Clop (79), underscoring sustained extortion pressure. Healthcare, education, and manufacturing sectors remained primary targets, as threat actors combined newly disclosed flaws with long-standing vulnerabilities to establish access, exfiltrate data, and maximize operational disruption.

Vulnerabilities added to the CISA KEV catalog in February 2026

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by malware	OSS
CVE-2026-1731	BeyondTrust	Remote Support (RS) and Privileged Remote Access (PRA)	OS Command Injection vulnerability in BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) that could result in remote code execution.	No	No	False
CVE-2026-2441	Google	Chromium	Use-After-Free vulnerability in Google Chromium CSS that enables a remote attacker to potentially exploit heap corruption via a crafted HTML page.	Yes	No	False
CVE-2026-20127	Cisco	Catalyst SD-WAN Controller and Manager	Authentication Bypass vulnerability in Cisco Catalyst SD-WAN Controller and Manager that enables an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system.	Yes	Yes	False
CVE-2026-20700	Apple	• iOS • macOS • tvOS	Buffer Overflow vulnerability in Apple multiple products that	Yes	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by malware	OSS
		• watchOS • visionOS	enables an attacker with memory write the capability to execute arbitrary code.			
CVE-2026-21510	Microsoft	Windows	Protection Mechanism Failure vulnerability in Microsoft Windows that enables an unauthorized attacker to bypass a security feature over a network.	Yes	No	False
CVE-2026-21513	Microsoft	Windows	Protection Mechanism Failure vulnerability in Microsoft MSHTML that enables an unauthorized attacker to bypass a security feature over a network.	Yes	No	False
CVE-2026-21514	Microsoft	Office	Reliance on Untrusted Inputs in a Security Decision vulnerability in Microsoft Office Word that enables an authorized attacker to elevate privileges locally.	Yes	No	False
CVE-2026-21519	Microsoft	Windows	Type Confusion vulnerability in Microsoft Windows that enables an authorized attacker to elevate privileges locally.	Yes	No	False
CVE-2026-21525	Microsoft	Windows	NULL Pointer Dereference vulnerability in Microsoft Windows that enables an unauthorized attacker to deny services locally.	Yes	No	False
CVE-2026-21533	Microsoft	Windows	Improper Privilege Management vulnerability in Microsoft Windows that enables an authorized attacker to elevate privileges locally.	Yes	No	False
CVE-2026-22769	Dell	RecoverPoint for Virtual Machines (RP4VMs)	Use of Hard-coded Credentials vulnerability in Dell RecoverPoint for Virtual Machines (RP4VMs) that enables unauthenticated remote attacker to gain unauthorized access to the underlying operating system and root-level persistence.	Yes	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by malware	OSS
CVE-2026-24423	SmarterTools	SmarterMail	Missing Authentication for Critical Function vulnerability in SmarterTools SmarterMail that could allow the attacker to point the SmarterMail instance to a malicious HTTP server which serves the malicious OS Command and could lead to command execution.	No	Yes	False
CVE-2026-25108	Soliton Systems K.K	FileZen	OS Command Injection vulnerability in Soliton Systems K.K when an user logs-in to the affected product and sends a specially crafted HTTP request.	No	No	False
CVE-2025-11953	React Native Community	CLI	OS Command Injection vulnerability in React Native Community CLI Metro Development Server that allows unauthenticated network attackers to send POST requests and run arbitrary executables via a vulnerable endpoint exposed by the server.	No	No	True
CVE-2025-15556	Notepad++	Notepad++	Download of Code Without Integrity Check vulnerability in Notepad++ that enables an attacker to intercept or redirect update traffic to download and execute an attacker-controlled installer.	No	Yes	False
CVE-2025-40536	SolarWinds	Web Help Desk	Security Control Bypass vulnerability in SolarWinds Web Help Desk that enables an unauthenticated attacker to gain access to certain restricted functionality.	No	No	False
CVE-2025-40551	SolarWinds	Web Help Desk	Deserialization of Untrusted Data vulnerability in SolarWinds Web Help Desk that could lead to remote code execution.	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by malware	OSS
CVE-2025-49113	Roundcube	Webmail	Deserialization of Untrusted Data vulnerability in RoundCube Webmail that enables remote code execution by authenticated users.	No	Yes	True
CVE-2025-64328	Sangoma	FreePBX	OS Command Injection vulnerability in Sangoma FreePBX that could allow for a post-authentication command injection by an authenticated known user via the ***testconnection*** -> ***check_ssh_connect()*** function.	No	Yes	False
CVE-2025-68461	Roundcube	Webmail	Cross-site Scripting vulnerability in RoundCube Webmail via the animate tag in an SVG document.	No	No	False
CVE-2024-7694	TeamT5	ThreatSonar Anti-Ransomware	Unrestricted Upload of File with Dangerous Type vulnerability in TeamT5 ThreatSonar Anti-Ransomware that allows remote attackers with administrative privileges on the platform to upload malicious files capable of executing arbitrary system commands on the underlying server.	No	No	False
CVE-2024-43468	Microsoft	Configuration Manager	SQL Injection vulnerability in Microsoft Configuration Manager that enables an unauthenticated attacker to exploit this vulnerability by sending specially crafted requests to target environment which are processed in an unsafe manner enabling the attacker to execute commands on the server and/or underlying database.	No	No	False
CVE-2022-20775	Cisco	SD-WAN	Path Traversal vulnerability in Cisco SD-WAN enables an authenticated local attacker to gain elevated privileges via improper access controls on	No	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by malware	OSS
			commands within the application CLI.			
CVE-2021-22175	GitLab	GitLab	A Server-Side Request Forgery vulnerability in GitLab that arises when requests to the internal network for webhooks are enabled.	No	No	False
CVE-2021-39935	GitLab	Community and Enterprise Editions	A Server-Side Request Forgery (SSRF) vulnerability in GitLab Community and Enterprise Editions that could allow unauthorized external users to perform Server Side requests via the CI lint API.	No	No	False
CVE-2020-7796	Synacor	Zimbra Collaboration Suite	A Server-Side Request Forgery vulnerability in Synacor Zimbra Collaboration Suite (ZCS) that arises when the WebEx zimlet is installed and zimlet JSP is enabled.	No	No	False
CVE-2019-19006	Sangoma	FreePBX	An Improper Authentication vulnerability in Sangoma FreePBX that potentially allows unauthorized users to bypass password authentication and access services provided by the FreePBX admin.	No	Yes	False
CVE-2008-0015	Microsoft	Windows	Remote Code Execution vulnerability in Microsoft Windows Video ActiveX Control allows attackers to execute arbitrary code by luring users to a specially crafted web page.	No	Yes	False

Actively Exploited Vulnerabilities in February 2026

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by malware	OSS
CVE-2026-21509	Microsoft	Office	Security Feature Bypass vulnerability in Microsoft Office that allows an unauthorized attacker to bypass a security feature locally.	Yes	Yes	False
CVE-2025-8088	RARLAB	WinRAR	Path Traversal vulnerability in RARLAB WinRAR that enables an attacker to execute arbitrary code by crafting malicious archive files.	No	Yes	False
CVE-2025-61155	Hotta Studio	GameDriverX64.sys	Access Control vulnerability in the GameDriverX64.sys kernel-mode anti-cheat driver that resides in the IOCTL handler, allows a user-mode process to obtain a handle to the driver device and submit specially crafted IOCTL requests.	Yes	Yes	False
CVE-2025-68947	NSecsoft	NSecKrnl	Missing Authorization vulnerability in NSecsoft NSecKrnl Windows driver	No	Yes	False
CVE-2019-11580	Atlassian	Crowd and Crowd Data Center	Remote Code Execution vulnerability in Atlassian Crowd and Crowd Data Center	No	Yes	False
CVE-2018-0802	Microsoft	Office	Memory Corruption vulnerability in Microsoft Office due to the way objects are handled in memory.	Yes	Yes	False
CVE-2010-1173	Linux	Kernel	Denial-of-Service vulnerability in Linux kernal	No	Yes	True
CVE-2010-2959	Linux	Kernel	Integer overflow vulnerability in Linux kernel	No	Yes	True
CVE-2010-3437	Linux	Kernel	NULL Pointer Dereference vulnerability in Linux kernel	No	Yes	True
CVE-2010-3849	Linux	Kernel	Denial-Of-Service vulnerability in Linux Kernel	No	Yes	True

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by malware	OSS
CVE-2009-2267	Broadcom	VMware	Path Traversal vulnerability in VMware Multiple Products	No	Yes	False
CVE-2009-2692	Linux	Kernel	NULL Pointer Dereference vulnerability in Linux Kernel	No	Yes	True
CVE-2009-2698	Linux	Kernel	NULL Pointer Dereference vulnerability in Linux Kernel	No	Yes	True
CVE-2009-2908	Linux	Kernel	Denial of Service vulnerability in Linux kernel	No	Yes	True
CVE-2009-3547	Linux	Kernel	Race Condition vulnerability in Linux kernel	No	Yes	True

Ransomware Insights for February 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 February 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.	110	• Manufacturing • Healthcare • Technology • Business Services • Financial Services	• CVE-2025-31324 • CVE-2024-21762 • CVE-2024-55591 • CVE-2023-27532

Ransomware	Description	No of affected organizations in February 2026	Targeted Industries	Vulnerabilities abused most
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.	83	• Manufacturing • Technology • Healthcare • Financial Services • Education	CVE-2025-7771
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,	79	• 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 February 2026	Targeted Industries	Vulnerabilities abused most
	making it both disruptive and coercive.			
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.	47	• 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
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.	39	• Healthcare • Technology • Business Services • Manufacturing • Education	• CVE-2023-3519 • CVE-2023-4966 • CVE-2023-48788
Dragonforce	DragonForce is a ransomware group originating from Malaysia. Initially, known as a hacktivist group, DragonForce has	34	• Manufacturing • Business Services	• CVE-2024-57726 • CVE-2024-57727 • CVE-2024-57728

Ransomware	Description	No of affected organizations in February 2026	Targeted Industries	Vulnerabilities abused most
	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.		• Technology • Healthcare • Construction	• CVE-2022-26134
Play	Play ransomware (aka Playcrypt), first observed in mid-2022, is a highly disruptive ransomware family known for its multi-extortion strategy, combining data encryption with threats of public data leaks on TOR-based sites. The group primarily gains initial access through vulnerability exploitation and exposed or rented RDP servers, with a notable focus on Fortinet FortiOS flaws and ProxyNotShell exploits. Once inside, Play emphasizes stealth and evasion, heavily leveraging LOLBins, COTS tools, intermittent encryption, and Active Directory abuse via GPOs to spread laterally. Its use of specialized tools like Grixba and AlphaVSS, along with commodity frameworks such as Cobalt Strike and Mimikatz, highlights a mature, operationally disciplined ransomware operation capable of targeting governments, enterprises, and critical institutions worldwide.	32	• Manufacturing • Business Services • Technology • Construction • Logistics	• CVE-2024-57727 • CVE-2022-41040 • CVE-2022-41080 • CVE-2022-41082 • CVE-2021-34523 • CVE-2020-12812 • CVE-2018-13379
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,	30	• Manufacturing • Healthcare • Technology • Business services • Consumer services	CVE-2024-55591

Ransomware	Description	No of affected organizations in February 2026	Targeted Industries	Vulnerabilities abused most
	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.			
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.	18	• Healthcare • Manufacturing • Construction • Technology • Business Services	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	12	• Healthcare • Technology • Business Services • Manufacturing • Financial Services	Unknown

Ransomware	Description	No of affected organizations in February 2026	Targeted Industries	Vulnerabilities abused most
	to pivot between direct extortion and the sale of access to maximize profits based on the target's profile.			

Conclusion

February's threat activity makes one point unmistakably clear: adversaries are optimizing speed, scale, and precision. From enterprise software exploitation to sustained ransomware campaigns targeting healthcare, education, and manufacturing, attackers are blending fresh disclosures with older weaknesses to maximize operational impact. Reactive patching is no longer sufficient in an environment where exploitation timelines continue to shrink. Organizations require continuous visibility into active threats, exploitation patterns, and sector-specific risk exposure. **Loginsoft Vulnerability Intelligence (LOVI)** empowers security teams to anticipate, prioritize, and respond with clarity transforming threat intelligence into decisive defensive action.