loginsoft

Monthly Report

Threat & Vulnerabilities Report – March 2026

Executive Summary

March 2026 witnessed heightened cybersecurity activity across the threat landscape, with continued exploitation of critical vulnerabilities, increased ransomware operations, and multiple high-impact disclosures affecting widely used technologies.

A total of 26 vulnerabilities were added to the Cybersecurity and Infrastructure Security Agency KEV catalog, underscoring real-world exploitation trends. Apple Inc. accounted for the highest number of entries, followed by Google and Microsoft, along with other vendors such as Craft CMS, Ivanti, Broadcom, Qualcomm, Langflow, Laravel, and SolarWinds.

Beyond KEV additions, active exploitation activity was observed across multiple platforms, including vulnerabilities in Apple Inc. products identified by Google and linked to advanced exploit chains such as the Coruna exploit kit. Additionally, Fortinet products were targeted in campaigns attributed to MuddyWater, as disclosed by Ctrl-Alt-Intel Threat Research.

Ransomware activity remained highly active, with groups like Qilin ransomware leading with 131 affected organizations, followed by Akira ransomware (71) and NightSpire ransomware (57). Other prominent actors, including DragonForce ransomware and IncRansom ransomware, also ranked among the top five, highlighting sustained ransomware pressure across sectors.

Vulnerabilities added to the CISA KEV catalog in March 2026

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2026-1603	Ivanti	Endpoint Manager (EPM)	Authentication Bypass vulnerability in Ivanti Endpoint Manager (EPM) that could allow a remote unauthenticated attacker to leak specific stored credential data.	No	No	False
CVE-2026-3055	Citrix	NetScaler	Out-of-Bounds Read vulnerability in Citrix NetScaler when configured as a SAML IDP leading to memory overread.	No	No	False
CVE-2026-3909	Google	Skia	Out-of-Bounds Write vulnerability in Google Skia could allow a remote attacker to perform out of bounds memory access via a crafted HTML page.	Yes	No	False
CVE-2026-3910	Google	Chromium V8	Improper Restriction of Operations Within the Bounds of a Memory Buffer vulnerability in Google Chromium V8 that could allow a remote attacker to execute arbitrary code inside	Yes	No	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			a sandbox via a crafted HTML page.			
CVE-2026-20131	Cisco	Secure Firewall Management Center (FMC)	Deserialization of Untrusted Data Vulnerability in Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management that could allow an unauthenticated, remote attacker to execute arbitrary Java code as root on an affected device.	Yes	Yes	False
CVE-2026-20963	Microsoft	SharePoint	Deserialization of Untrusted Data vulnerability in Microsoft SharePoint allows an unauthorized attacker to execute code over a network.	No	No	False
CVE-2026-21385	Qualcomm	Multiple Chipsets	Memory Corruption vulnerability in Qualcomm multiple chipsets while using alignments for memory allocation.	No	No	True
CVE-2026-22719	Broadcom	VMware Aria Operations	Command Injection vulnerability in Broadcom VMware Aria Operations allows an unauthenticated attacker to execute arbitrary commands.	No	No	False
CVE-2026-33017	Langflow	Langflow	Code Injection vulnerability in Langflow could allow building public flows without requiring authentication.	No	No	True
CVE-2026-33634	Aquasecurity	Trivy	Embedded Malicious Code vulnerability in Aquasecurity Trivy that could allow an attacker to gain access to everything in the CI/CD environment, including all tokens, SSH keys, cloud credentials, database passwords, and any sensitive configuration in memory.	No	Yes	False
CVE-2025-26399	SolarWinds	Web Help Desk	Deserialization of Untrusted Data vulnerability in SolarWinds Web Help Desk in AjaxProxy that could allow an attacker to run commands on the host machine.	No	No	False
CVE-2025-31277	Apple	Multiple Products	Buffer Overflow vulnerability in Apple Multiple Products could allow the processing of	Yes	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			maliciously crafted web content which may lead to memory corruption.			
CVE-2025-32432	Craft CMS	Craft CMS	Code Injection vulnerability in Craft CMS allows a remote attacker to execute arbitrary code.	Yes	Yes	True
CVE-2025-43510	Apple	Multiple Products	Improper Locking vulnerability in Apple Multiple Products could allow a malicious application to cause unexpected changes in memory shared between processes.	Yes	Yes	False
CVE-2025-43520	Apple	Multiple Products	Classic Buffer Overflow vulnerability in Apple Multiple Products could allow a malicious application to cause unexpected system termination or write kernel memory.	Yes	Yes	False
CVE-2025-47813	Wing FTP Server	Wing FTP Server	Information Disclosure vulnerability in Wing FTP Server when using a long value in the UID cookie.	No	No	False
CVE-2025-53521	F5	BIG-IP	Remote Code Execution vulnerability In F5 BIG-IP APM.	No	No	False
CVE-2025-54068	Laravel	Livewire	Code Injection vulnerability in Laravel Livewire could allow unauthenticated attackers to achieve remote command execution in specific scenarios.	No	Yes	True
CVE-2025-66376	Synacor	Zimbra Collaboration Suite (ZCS)	Cross-Site Scripting vulnerability in Synacor Zimbra Collaboration Suite (ZCS) in the Classic UI where attackers could abuse Cascading Style Sheets (CSS) @import directives in email HTML.	No	Yes	False
CVE-2025-68613	n8n	n8n	Improper Control of Dynamically-Managed Code Resources vulnerability in n8n in its workflow expression evaluation system that allows for remote code execution.	No	Yes	False
CVE-2023-41974	Apple	• iOS • iPadOS	Use-After-Free vulnerability in Apple iOS and iPadOS that might enable an app to	Yes	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			execute arbitrary code with kernel privileges.			
CVE-2023-43000	Apple	Multiple Products	Use-After-Free vulnerability in Apple multiple products due to the processing of maliciously crafted web content that may lead to memory corruption.	Yes	Yes	False
CVE-2021-22054	Omnissa	Workspace One UEM	Server-Side Request Forgery vulnerability in Omnissa Workspace ONE that could allow a malicious actor with network access to UEM to send their requests without authentication and to gain access to sensitive information.	No	No	False
CVE-2021-22681	Rockwell	Multiple Products	Insufficient Protected Credentials vulnerability in Rockwell multiple products.	Yes	No	False
CVE-2021-30952	Apple	Multiple Products	Integer Overflow or Wraparound vulnerability in Apple multiple products due to the processing of maliciously crafted web content that can lead to arbitrary code execution.	Yes	Yes	True
CVE-2017-7921	Hikvision	Multiple Products	Improper Authentication vulnerability in Hikvision multiple products allows a malicious user to escalate privileges on the system and gain access to sensitive information.	No	Yes	False

Actively Exploited Vulnerabilities in March 2026

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2026-0953	Tutor LMS	Pro plugin for WordPress	An Authentication Bypass vulnerability in the Tutor LMS Pro plugin for WordPress via the Social Login Addon.	No	No	False
CVE-2026-1281	Ivanti	Endpoint Manager Mobile (EPMM)	Code Injection vulnerability in Ivanti Endpoint Manager Mobile (EPMM) allows attackers to achieve unauthenticated remote code execution.	No	Yes	False

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).	No	Yes	False
CVE-2026-3502	TrueConf	Client video conferencing software	Download of Code Without Integrity Check vulnerability in TrueConf client video conferencing software that allows an attacker to distribute a tampered update, resulting in the execution of arbitrary code.	Yes	Yes	False
CVE-2026-3584	WP Chill	Kali Forms Plugin	Unauthenticated Remote Code Execution vulnerability in Kali Forms Plugin	No	No	False
CVE-2026-20700	Apple	Multiple products	Buffer Overflow vulnerability in Apple multiple products.	Yes	Yes	False
CVE-2026-28353	Trivy	Vulnerability Scanner	Information Disclosure vulnerability in Trivy Vulnerability Scanner VS Code extension.	No	Yes	False
CVE-2025-5777	Citrix	NetScaler ADC and Gateway	Out-of-Bounds Read vulnerability in Citrix NetScaler ADC and Gateway.	Yes	Yes	False
CVE-2025-9316	N-able	N-central	Improper Access Control vulnerability in N-central.	Yes	Yes	False
CVE-2025-14174	Google	Chromium	Out of Bounds Memory Access vulnerability in Google Chromium.	Yes	Yes	False
CVE-2025-32975	Quest	KACE Systems Management Appliance	Authentication Bypass vulnerability in Quest KACE Systems Management Appliance (SMA) that enables attackers to impersonate legitimate users without valid credentials.	No	No	False
CVE-2025-34291	Langflow	Langflow	Remote Code Execution vulnerability in Langflow.	No	Yes	True
CVE-2025-43529	Apple	Multiple products	Memory Corruption vulnerability in Apple multiple products.	Yes	Yes	False
CVE-2025-52691	SmarterTools	SmarterMail	Unrestricted Upload of File with Dangerous Type vulnerability in SmarterTools SmarterMail.	No	Yes	False
CVE-2025-55182	Meta	React Server	Remote Code Execution vulnerability in Meta React Server Components.	Yes	Yes	True

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2024-4577	PHP	CGI	OS Command Injection vulnerability in PHP CGI leads to remote code execution.	No	Yes	False
CVE-2024-23113	Fortinet	Multiple products	Format String vulnerability in Fortinet Multiple Products.	No	Yes	False
CVE-2024-23222	Apple	Multiple products	Type Confusion vulnerability in Apple multiple products can lead to code execution when processing maliciously crafted web content.	Yes	Yes	True
CVE-2024-23225	Apple	Multiple products	Memory Corruption vulnerability in Apple multiple products enables attacker with arbitrary kernel read and write capability to bypass kernel memory protections.	Yes	Yes	False
CVE-2024-23296	Apple	Multiple products	Memory Corruption vulnerability in Apple multiple products enables an attacker with arbitrary kernel read and write capability to bypass kernel memory protections.	Yes	Yes	False
CVE-2024-55591	Fortinet	FortiOS and FortiProxy	Authentication Bypass vulnerability in Fortinet FortiOS and FortiProxy.	Yes	Yes	False
CVE-2022-42475	Fortinet	FortiOS and FortiProxy	Heap-based Buffer Overflow vulnerability in FortiOS SSL-VPN and FortiProxy SSL-VPN.	Yes	Yes	False
CVE-2023-32409	Apple	Multiple products	Sandbox Escape vulnerability in Apple multiple products enable a remote attacker to break out the Web Content sandbox.	Yes	Yes	False
CVE-2023-38606	Apple	Multiple products	Unspecified vulnerability in Apple multiple products that allow an app to modify a sensitive kernel state.	Yes	Yes	False
CVE-2022-48503	Apple	Multiple products	Unspecified vulnerability in Apple multiple products in the JavaScriptCore when processing web content may lead to arbitrary code execution.	Yes	Yes	True
CVE-2020-27932	Apple	Multiple products	Type Confusion vulnerability in Apple multiple products that may	Yes	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			allow a malicious application to execute code with kernel privileges.			
CVE-2020-27950	Apple	Multiple products	Memory Initialization vulnerability in Apple multiple products that may allow a malicious application to disclose kernel memory.	Yes	Yes	False

Ransomware Insights for March 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 March 2026	Targeted Industries	Vulnerabilities abused most
Qilin	Qilin ransomware, first observed in 2022. It often gains initial access through compromised RDP credentials. Once inside, Qilin quietly spreads laterally across the network, encrypting files and disabling security measures. Its notable features include its ability to evade detection, self-propagate, and negotiate ransom payments through a dedicated Tor-based website.	131	• Manufacturing • Healthcare • Technology • Business Services • Financial Services	• CVE-2025-31324 • CVE-2024-21762 • CVE-2024-55591 • CVE-2023-27532
Akira	Akira ransomware, first seen in 2023, encrypts files on infected systems and demands a ransom for decryption. It employs double extortion tactics, threatening to release stolen data if the ransom isn't paid. Akira spreads primarily through phishing emails and exploits weak network security protocols. The ransomware targets various industries, including the airline sector in LATAM. It uses advanced encryption techniques and evades detection by disabling recovery options, making it challenging for victims to restore their data without paying the ransom.	71	• 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
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	57	• Manufacturing • Healthcare • Technology • Business services	CVE-2024-55591

Ransomware	Description	No of affected organizations in March 2026	Targeted Industries	Vulnerabilities abused most
	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.		• Consumer services	
Dragonforce	First discovered in 2023, DragonForce is a ransomware strain that targets various organizations by encrypting their files and demanding a ransom for decryption. It is known for employing highly sophisticated techniques, including exploiting vulnerabilities and leveraging malware-as-a-service platforms. Often linked to cybercriminal groups, DragonForce attacks both public and private sectors and continues to evolve with each incident.	56	• Manufacturing • Technology • Business Services • Construction • Healthcare	• CVE-2024-57726 • CVE-2024-57727 • CVE-2024-57728 • CVE-2022-26134
IncRansom	INC Ransomware was first observed in early 2023, primarily targeting healthcare organizations. Initially, it gained access through phishing emails containing malicious attachments or links. Its behavior included disabling backups and spreading through the network, making recovery difficult without paying.	50	• Healthcare • Technology • Business Services • Manufacturing • Education	• CVE-2023-3519 • CVE-2023-4966 • CVE-2023-48788
Thegentlemen	The Gentlemen ransomware campaign, which surfaced in the summer of 2025, exemplifies the rapid evolution of modern cyber threats. It combines advanced techniques with persistent, targeted operations, leveraging custom defense-evasion tools, adapting to existing security controls, and exploiting both legitimate and vulnerable components to effectively bypass layered defenses. The Gentlemen operators aggressively target and terminate critical services related to backup, database, and security operations, maximizing operational disruption and impact.	48	• Manufacturing • Technology • Healthcare • Financial Services • Education	CVE-2025-7771
LockBit5	LockBit 5.0, internally codenamed ChuongDong, was announced on the	46	• Technology	Unknown

Ransomware	Description	No of affected organizations in March 2026	Targeted Industries	Vulnerabilities abused most
	RAMP dark web forum in September 2025 to mark the group's six-year anniversary, resuming operations after the February 2024 Operation Cronos law enforcement takedown. LockBit 5.0 payloads are built with a leaked version of the LockBit 3.0 builder and subsequently packed and 'branded' as a new variant of LockBit. LockBit 5.0 ransom notes instruct the victim to communicate with the attacker via TOX messenger.		• Manufacturing • Healthcare • Education • Public Sector	
Handala	The Handala ransomware campaign showcases a highly targeted attack on Israeli infrastructure, leveraging advanced social engineering to deploy cross-platform data-wiping malware. The attack employed a multi-stage loader chain, including obfuscated scripts, a Delphi-based second-stage loader, and an AutoIt injector, ransom demands, and defacement of websites, not only highlight their technical proficiency but also their ideological motivations.	38	• Technology • Government • Energy • Healthcare • Public Sector	Unknown
Play	Play ransomware was first seen in June 2022, targeting organizations through various initial access methods, such as exploiting vulnerabilities in Remote Desktop Protocol (RDP). It collects sensitive data and encrypts files, demanding ransom for decryption. Play has impacted multiple industries, including healthcare and finance, with significant activity observed in the U.S and Europe.	33	• 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
Anubis	Anubis is a Ransomware-as-a-Service (RaaS) operation distributed via spearphishing, featuring both file encryption and an optional wipe mode that enables permanent data destruction. This dual-threat capability allows attackers to erase files if ransom demands are unmet, increasing pressure on victims. Its affiliate program supports flexible revenue sharing and additional monetization tactics such as data extortion and access sales.	8	• Healthcare • Manufacturing • Business Services • Technology • Hospitality and Tourism	Unknown

Conclusion

March 2026 underscored a stark reality in the global threat landscape, adversaries are no longer waiting for exploits to mature. the month demonstrated the breadth and velocity at which threat actors are weaponizing disclosed vulnerabilities, often within hours of advisory publication. The DarkSword iOS exploit chain, the TeamPCP supply chain campaign, and active exploitation of platforms from Apple, Citrix, Quest, and others collectively illustrated that no technology stack, vendor, or deployment model is beyond the reach of sophisticated adversaries whether state-sponsored espionage groups, commercial surveillance vendors, or financially motivated threat actors. Leveraging platforms like **Loginsoft Vulnerability Intelligence (LOVI)** enables organizations to track actively exploited vulnerabilities, prioritize risks, and respond effectively to evolving threat activity.