loginsoft

Monthly Report

Threat & Vulnerabilities Report – April 2026

Executive Summary

April 2026 highlighted a threat landscape where recency no longer defines risk, as both newly disclosed and long-standing vulnerabilities were actively leveraged across diverse environments. The Cybersecurity and Infrastructure Security Agency added 31 vulnerabilities to its KEV catalog, spanning major vendors such as Microsoft, Cisco, Fortinet, Adobe, Google, and others, including flaws dating back to 2012 and 2009. This mix of legacy and current vulnerabilities underscores persistent exposure in unpatched systems and the continued effectiveness of older exploits.

In parallel, active exploitation was observed across a wide range of platforms, including widely used web applications, open-source tools, AI frameworks, and network devices such as Ninja Forms, Qinglong, Oracle products, Weaver, MajorDoMo, Nginx-ui, LMDeploy, LiteLLM, ShowDoc, Flowise AI, TP-Link, TBK, and Huawei systems. The breadth of affected technologies reflects a rapidly expanding attack surface, where attackers are simultaneously exploiting enterprise software, developer tools, and IoT infrastructure.

Ransomware activity remained consistently high throughout the month, with Qilin ransomware leading with 98 affected organizations, followed by Thegentlemen ransomware (75), DragonForce ransomware (63), and Akira ransomware (47). Additional activity from groups such as LockBit5, IncRansom, and NightSpire ransomware further contributed to the overall threat volume, underscoring sustained pressure across multiple sectors. The distribution of incidents highlights continued operational momentum among both established and emerging ransomware groups, reinforcing the persistence of financially motivated attacks.

Vulnerabilities added to the CISA KEV catalog in April 2026

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2026-1340	Ivanti	Endpoint Manager Mobile (EPMM)	Code Injection vulnerability in Ivanti Endpoint Manager Mobile (EPMM) that could allow attackers to achieve unauthenticated remote code execution.	Yes	No	False
CVE-2026-3502	TrueConf	Client	Download of Code Without Integrity Check vulnerability in TrueConf Client that can result in arbitrary code execution in the context of the updating process or user.	Yes	No	False
CVE-2026-5281	Google	Dawn	Use-After-Free vulnerability in Google Dawn that could allow a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.	Yes	No	False
CVE-2026-20122	Cisco	Catalyst SD-WAN Manger	Incorrect Use of Privileged APIs vulnerability in Cisco	Yes	No	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			Catalyst SD-WAN Manager due to improper file handling on the API of an affected system.			
CVE-2026-20128	Cisco	Catalyst SD-WAN Manager	Storing Passwords in a Recoverable Format vulnerability in Cisco Catalyst SD-WAN Manager that allows an authenticated, local attacker to gain DCA user privileges by accessing a credential file for the DCA user on the filesystem as a low-privileged user.	Yes	No	False
CVE-2026-20133	Cisco	Catalyst SD-WAN Manger	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Cisco Catalyst SD-WAN Manager that could allow remote attackers to view sensitive information on affected systems.	Yes	No	False
CVE-2026-21643	Fortinet	FortiClient EMS	SQL Injection vulnerability in Fortinet FortiClient EMS that may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	No	No	False
CVE-2026-32201	Microsoft	SharePoint Server	Improper Input Validation vulnerability in Microsoft SharePoint Server that allows an unauthorized attacker to perform spoofing over a network.	Yes	No	False
CVE-2026-32202	Microsoft	Windows	Protection Mechanism Failure Vulnerability in Microsoft Windows that allows an unauthorized attacker to perform spoofing over a network.	No	No	False
CVE-2026-33825	Microsoft	Defender	Insufficient Granularity of Access Control vulnerability in Microsoft Defender that could allow an authorized attacker to escalate privileges locally.	No	No	False
CVE-2026-34197	Apache	ActiveMQ	Improper Input Validation vulnerability in Apache ActiveMQ that allows for code injection.	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2026-34621	Adobe	Acrobat and Reader	Prototype Pollution vulnerability in Adobe Acrobat and Reader that allows for arbitrary code execution.	Yes	No	False
CVE-2026-35616	Fortinet	FortiClient EMS	Improper Access Control vulnerability in Fortinet FortiClient EMS that may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests.	Yes	No	False
CVE-2026-39987	Marimo	Marimo	Remote Code Execution vulnerability in Marimo allowing an unauthenticated attacked to shell access and execute arbitrary system commands.	No	Yes	True
CVE-2026-41940	WebPros	cPanel & WHM and WP2 (WordPress Squared)	Missing Authentication for Critical Function Vulnerability in WebPros cPanel & WHM and WP2 (WordPress Squared) that allows unauthenticated remote attackers to gain unauthorized access to the control panel.	No	No	False
CVE-2025-2749	Kentico	Kentico Xperience	Path Traversal vulnerability in Kentico Xperience that could allow an authenticated user's Staging Sync Server to upload arbitrary data to path relative locations.	No	No	False
CVE-2025-29635	D-Link	DIR-823X	Command Injection vulnerability in D-Link DIR-823X that allows an authorized attacker to execute arbitrary commands on remote devices by sending a POST request to ***/goform/set_prohibiting*** via the corresponding function.	No	Yes	False
CVE-2025-32975	Quest	KACE Systems Management Appliance (SMA)	Improper Authentication vulnerability in Quest KACE Systems Management Appliance (SMA) that could allow attackers to impersonate legitimate users without valid credentials.	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2025-48700	Synacor	Zimbra Collaboration Suite (ZCS)	Cross-site Scripting vulnerability in Synacor Zimbra Collaboration Suite that could allow attackers to execute arbitrary JavaScript within the user's session, potentially leading to unauthorized access to sensitive information.	No	No	False
CVE-2025-60710	Microsoft	Windows	Link Following vulnerability in Microsoft Windows that allows for privilege escalation.	No	No	False
CVE-2024-1708	ConnectWise	ScreenConnect	Path Traversal vulnerability in ConnectWise SreenConnect allows an attacker to execute remote code or directly impact confidential data and critical systems.	No	Yes	False
CVE-2024-7399	Samsung	MagicINFO 9 Server	Path Traversal vulnerability in Samsung MagicINFO 9 Server that could allow an attacker to write arbitrary files as system authority.	No	Yes	False
CVE-2024-27199	JetBrains	TeamCity	Relative Path Traversal vulnerability in JetBrains TeamCity that could allow limited admin actions to be performed.	Yes	Yes	False
CVE-2024-57726	SimpleHelp	SimpleHelp	Missing Authorization vulnerability in SimpleHelp that could allow low-privileged technicians to create API keys with excessive permissions.	No	Yes	False
CVE-2024-57728	SimpleHelp	SimpleHelp	Path Traversal vulnerability in SimpleHelp that allows admin users to upload arbitrary files anywhere on the file system by uploading a crafted zip file (i.e. zip slip).	No	Yes	False
CVE-2023-21529	Microsoft	Exchange Server	Deserialization of Untrusted Data vulnerability in Microsoft Exchange Server that allows an authenticated attacker to achieve remote code execution.	Yes	Yes	False
CVE-2023-27351	PaperCut	NG/MF	Improper Authentication vulnerability in PaperCut NG/MF that could allow remote attackers to bypass authentication on affected	No	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			installations via the SecurityRequestFilter class.			
CVE-2023-36424	Microsoft	Windows	Out-of-Bounds Read vulnerability in Microsoft Windows Common Log File System Driver that could allow a threat actor for privileges escalation.	No	No	False
CVE-2020-9715	Adobe	Acrobat	Use-After-Free vulnerability in Adobe Acrobat that allows for code execution.	No	No	False
CVE-2012-1854	Microsoft	Visual Basic for Applications (VBA)	Insecure Library Loading Vulnerability in Microsoft Visual Basic for Applications that could allow for remote code execution.	No	No	False
CVE-2009-0238	Microsoft	Office	Remote Code Execution in Microsoft Office that could allow an attacker to take complete control of an affected system if a user opens a specially crafted Excel file that includes a malformed object.	No	No	False

Actively Exploited Vulnerabilities in April 2026

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2026-0740	Ninja Forms	File Upload WordPress	Unauthenticated Arbitrary File Upload vulnerability in Ninja Forms- File Upload WordPress Plugin that can lead to remote code execution	No	No	False
CVE-2026-3965	Qinglong	Qinglong	Protection Mechanism Failure vulnerability in Qinglong exposes protected administrative endpoints through an authentication bypass caused by a misconfigured rewrite rule that maps /open/ requests to /api/.	Yes	No	False
CVE-2026-4047	Qinglong	Qinglong	Protection Mechanism Failure vulnerability in Qinglong arises from inconsistent path handling, where authentication checks	Yes	No	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			treat routes as case-sensitive (/api/) while the router processes them case-insensitively, allowing crafted requests such as /aPi/... to bypass authentication and access protected endpoints.			
CVE-2026-21962	Oracle	HTTP Server and WebLogic Server Proxy Plugin	Unauthenticated Remote Code Execution vulnerability in Oracle WebLogic Server that allows a specially crafted HTTP request to execute arbitrary operating system commands on the vulnerable server.	No	No	False
CVE-2026-22679	Weaver	E-cology	Remote Code Execution vulnerability in Weaver (Fanwei) E-cology in the /papi/esearch/data/devops/dubboApi/debug/method endpoint that allows attackers to execute arbitrary commands by invoking exposed debug functionality.	No	No	False
CVE-2026-27174	MajorDoMo	MajorDoMo	Remote Code Execution vulnerability in the MajorDoMo that allows unauthenticated attackers to execute arbitrary PHP code via the admin panel.	No	No	False
CVE-2026-27175	MajorDoMo	MajorDoMo	Unauthenticated OS Command Injection vulnerability in MajorDoMo via rc/index.php.	No	No	False
CVE-2026-33032	Nginx-ui	Nginx-ui	Authentication Bypass vulnerability in Nginx-ui that enables threat actors to seize control of the Nginx service.	No	No	True
CVE-2026-33626	LMDeploy	LMDeploy	Server-Side Request Forgery in LMDeploy toolkit that allows attackers to access cloud metadata services, internal networks, and sensitive resources.	No	No	False
CVE-2026-42208	LiteLLM	LiteLLM	Pre-Authentication SQL Injection vulnerability in LiteLLM that could allow an attacker to read data from the proxy's database.	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2025-0520	ShowDoc	ShowDoc	Unrestricted Upload of File with Dangerous Type vulnerability in ShowDoc that enables an attacker to upload arbitrary PHP files and achieve remote code execution.	No	No	True
CVE-2025-59528	Flowise AI	Flowise AI	Remote Code Execution vulnerability in Flowise AI that can lead to full system compromise, file system access, command execution, and sensitive data exfiltration	No	No	True
CVE-2023-50224	TP-Link	TL-WR841N	Authentication Bypass by Spoofing vulnerability in TP-Link TL-WR841N within the httpd service, which listens on TCP port 80 by default, leading to the disclose of stored credentials.	No	Yes	False
CVE-2024-3721	TBK	DVR-4104 and DVR-4216	Command Injection vulnerability in TBK DVR-4104 and DVR-4216 up to 20240412	Yes	Yes	False
CVE-2017-17215	Huawei	HG532	Remote Code Execution vulnerability in Huawei HG532	No	Yes	False

Ransomware Insights for April 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 April 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.	98	• Manufacturing • Healthcare • Technology • Business Services • Financial Services	• CVE-2025-31324 • CVE-2024-21762 • CVE-2024-55591 • CVE-2023-27532
Thegentlemen	The Gentlemen ransomware campaign, which surfaced in the summer of 2025, exemplifies the rapid evolution of modern cyber threats. It combines	75	• Manufacturing • Technology • Healthcare	CVE-2025-7771

Ransomware	Description	No of affected organizations in April 2026	Targeted Industries	Vulnerabilities abused most
	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.		• Financial Services • Education	
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.	63	• Manufacturing • Technology • Business Services • Construction • Healthcare	• CVE-2024-57726 • CVE-2024-57727 • CVE-2024-57728 • CVE-2022-26134
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.	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
LockBit5	LockBit 5.0, internally codenamed ChuongDong, was announced on the 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	36	• Technology • Manufacturing • Healthcare • Education • Public Sector	Unknown

Ransomware	Description	No of affected organizations in April 2026	Targeted Industries	Vulnerabilities abused most
	communicate with the attacker via TOX messenger.			
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.	32	• Healthcare • Technology • Business Services • Manufacturing • Education	• CVE-2023-3519 • CVE-2023-4966 • CVE-2023-48788
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.	20	• Manufacturing • Healthcare • Technology • Business services • Consumer services	CVE-2024-55591
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.	9	• Healthcare • Manufacturing • Business Services • Technology • Hospitality and Tourism	Unknown
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.	8	• Technology • Government • Energy • Healthcare • Public Sector	Unknown

Ransomware	Description	No of affected organizations in April 2026	Targeted Industries	Vulnerabilities abused most
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.	3	• 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

Conclusion

April 2026 reinforced a critical shift in the threat landscape exploitation is no longer bound by vulnerability age, but by opportunity. The month demonstrated how adversaries actively leveraged both newly disclosed flaws and years-old weaknesses across enterprise platforms, developer tools, and IoT ecosystems. The expansion of the Cybersecurity and Infrastructure Security Agency KEV catalog alongside real-world exploitation in platforms such as Qinglong and LiteLLM highlighted a dual trend of rapid weaponization and persistent legacy risk. These developments emphasize that no environment whether modern AI infrastructure or aging network devices is beyond adversarial reach. Leveraging platforms like **Loginsoft Vulnerability Intelligence (LOVI)** enables organizations to track active threats, prioritize remediation, and respond with precision to an increasingly dynamic and converged threat landscape.