loginsoft

Monthly Report

Threat & Vulnerabilities Report – July 2026

Executive Summary

July 2026 closed out as a month defined by relentless pressure on internet-facing infrastructure, where attackers continued to favor known weaknesses in edge appliances, collaboration platforms, and enterprise software over novel techniques. The month's activity reinforced a familiar but sharpening reality, that the gap between disclosure and exploitation keeps narrowing, and that both state-aligned actors and financially motivated crews are moving faster to weaponize flaws before organizations can remediate.

CISA added 26 vulnerabilities to its Known Exploited Vulnerabilities catalog through July, spanning a broad cross-section of enterprise vendors. Microsoft led the additions with five entries, followed by Fortinet with three, and two apiece from SonicWall, WordPress, Cisco, and Langflow, alongside further entries affecting major vendors including Adobe, Check Point, and Oracle. The spread underscored that exploitation was not concentrated in any single technology, but distributed across operating systems, firewalls, VPN gateways, content management systems, and AI development frameworks, reflecting the widening attack surface defenders were forced to cover.

Beyond the KEV additions, active exploitation surfaced across a wide range of additional products throughout the month. Threat actors were observed targeting Citrix, Alibaba Fastjson, and multiple WordPress plugins, along with ASUS devices, Synacor Zimbra, and Ruckus Wireless products, demonstrating sustained interest in both widely deployed enterprise platforms and open-source components. This activity highlighted that exploitation extended well beyond cataloged vulnerabilities, with adversaries probing edge services and web-facing software for any foothold that could enable initial access or persistence.

The ransomware landscape remained highly active in July 2026, with Qilin emerging as the most prolific operation, claiming 124 victims over the month. TheGentlemen followed with 104 victims, and DragonForce accounted for 41, together reflecting a concentration of impact among a handful of aggressive, high-volume groups. The scale of these figures reinforced that ransomware continued to represent the most immediate and disruptive threat to organizations, with established operators maintaining steady operational tempo across multiple sectors.

Vulnerabilities added to the CISA KEV catalog in July 2026

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-0770	Langflow	Langflow	Inclusion of Functionality from Untrusted Control Sphere vulnerability in Langflow that allows remote attackers to execute arbitrary code on affected installations.	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-15409	SonicWall	SMA1000 Appliances	Server-Side Request Forgery vulnerability in SonicWall SMA1000 Appliances that could allow a remote unauthenticated attacker to potentially cause the appliance to make requests to unintended location.	Yes	Yes	False
CVE-2026-15410	SonicWall	SMA1000 Appliances	Code Injection vulnerability in SonicWall SMA1000 appliances which in specific conditions could potentially enable a remote authenticated attacker as administrator to execute arbitrary OS commands.	Yes	Yes	False
CVE-2026-16232	Check Point	SmartConsole	Improper Authentication vulnerability in Check Point SmartConsole which could allow an unauthenticated remote attacker to obtain an application login token and use it to authenticate with full administrative privileges.	Yes	No	False
CVE-2026-16812	Arista	VeloCloud Orchestrator	OS Command Injection vulnerability in Arista VeloCloud Orchestrator On-Prem that may allow a remote attacker to access privileged internal functionality and impact the VCO host. Successful exploitation may compromise the confidentiality, integrity, and availability of the orchestrator and data managed by the orchestrator.	Yes	No	False
CVE-2026-20316	Cisco	Secure Firewall Management Center (FMC)	Use of Hard-coded Password vulnerability in Cisco Secure Firewall Management Center that could allow an unauthenticated, remote attacker to log in to an affected device using a low-privileged account to access sensitive data within the impacted systems.	Yes	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-25089	Fortinet	FortiSandbox	OS Command Injection vulnerability in Fortinet FortiSandbox FortiSandbox Cloud, and FortiSandbox PaaS that allows an unauthenticated attacker to execute unauthorized commands via specifically crafted HTTP requests.	No	No	False
CVE-2026-39808	Fortinet	FortiSandbox	OS Command Injection vulnerability in Fortinet FortiSandbox that could allow an unauthenticated attacker to execute unauthorized code or commands via crafted HTTP requests.	No	No	False
CVE-2026-45659	Microsoft	SharePoint Server	Deserialization of Untrusted Data vulnerability in Microsoft SharePoint server which allows an authorized attacker to execute code over a network.	No	Yes	False
CVE-2026-46817	Oracle	E-Business Suite	Improper Privilege Management vulnerability in Oracle E-Business Suite that allows an unauthenticated attacker with network access via HTTP to compromise Oracle Payments.	No	No	False
CVE-2026-48282	Adobe	ColdFusion	Path Traversal vulnerability in Adobe ColdFusion that could lead to arbitrary code execution in the context of the current user.	No	No	False
CVE-2026-48908	JoomShaper	SP Page Builder	Unrestricted Upload of File with Dangerous Type vulnerability in JoomShaper SP Page Builder that allows unauthenticated users to upload arbitrary files, ultimately resulting in the upload and execution of PHP code.	Yes	No	False
CVE-2026-48939	iCagenda	iCagenda	Unrestricted Upload of File with Dangerous Type vulnerability in iCagenda that allows the upload of arbitrary files in the file attachment feature, ultimately resulting	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			in PHP code upload and execution.			
CVE-2026-50522	Microsoft	SharePoint	Deserialization of Untrusted Data vulnerability in Microsoft SharePoint vulnerability which could allow an unauthorized attacker to execute code over a network.	No	No	False
CVE-2026-55255	Langflow	Langflow	Authorization Bypass Through User-Controlled Key vulnerability in Langflow that allows an authenticated attacker to execute any flow belonging to another user by specifying the victim's flow ID in the request.	No	No	True
CVE-2026-56155	Microsoft	Active Directory Federation Services	Insufficient Granularity of Access Control vulnerability in Microsoft Active Directory Federation Services that allows an authorized attacker to elevate privileges locally.	Yes	No	False
CVE-2026-56164	Microsoft	SharePoint Server	Missing Authentication for Critical Function vulnerability in Microsoft SharePoint Server that allows an unauthorized attacker to elevate privileges over a network.	Yes	No	False
CVE-2026-56290	Joomlack	Page Builder	Improper Access Control vulnerability in Joomlack Page Builder that could allow for remote code execution via unauthenticated arbitrary file upload.	No	No	False
CVE-2026-56291	Balbooa	Forms	Unrestricted Upload of File with Dangerous Type vulnerability in Balbooa Forms that allows an unauthenticated arbitrary file upload which could allow uploading of files leading to full remote code execution.	No	No	False
CVE-2026-58644	Microsoft	SharePoint	Deserialization of Untrusted Data vulnerability in Microsoft SharePoint that allows an unauthorized attacker to execute code over a network.	Yes	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-60137	WordPress	Core	SQL Injection vulnerability in WordPress Core when a plugin or theme passes untrusted input to the parameter. This vulnerability can be chained with CVE-2026-63030 to allow an unauthenticated attacker to gain remote code execution on default WordPress installations.	No	No	False
CVE-2026-63030	WordPress	Core	Interpretation Conflict vulnerability in WordPress Core that could allow an attacker to perform SQL Injection and achieve Remote Code Execution. This vulnerability can be chained with CVE-2026-60137.	No	No	False
CVE-2025-68686	Fortinet	FortiOS	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Fortinet FortiOS that may allow a remote unauthenticated attacker to bypass the patch developed for the symbolic link persistency mechanism observed in some post-exploit cases, via crafted HTTP requests. An attacker would need first to have compromised the product via another vulnerability, at filesystem level.	No	No	False
CVE-2023-4346	KNX Association	KNX Protocol Connection Authorization Option 1	Overly Restrictive Account Lockout Mechanism vulnerability in KNX Association KNX Protocol Connection Authorization Option 1 that could allow an attacker to purge all devices without additional security options enabled and set a BCU key to lock the device.	No	No	False
CVE-2021-27137	DD-WRT	DD-WRT	Stack-Based Buffer Overflow Vulnerability in DD-WRT that could allow an unauthenticated attacker to overflow an internal buffer	No	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			used by UPnP and trigger a code execution vulnerability.			
CVE-2008-4128	Cisco	IOS	Cross-Site Request Forgery vulnerability in Cisco IOS that allows remote attackers to execute arbitrary commands via (1) a certain "show privilege" command to the /level/15/exec/- URI, and (2) a certain "alias exec" command to the /level/15/exec/-/configure/http URI.	No	Yes	False

Actively Exploited Vulnerabilities in July 2026

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2026-1207	The Django Software Foundation	Django	SQL Injection vulnerability in Django RasterField on PostGIS that allows attackers to inject SQL via band index parameter, potentially leading to unauthorized data access or manipulation.	No	No	True
CVE-2026-6875	ServiceNow	ServiceNow	Remote Code Execution vulnerability in ServiceNow Ai platform that allows unauthenticated attackers to escape the sandbox and execute code remotely within the platform.	No	No	False
CVE-2026-8451	Citrix	NetScaler ADC and NetScaler Gateway	Insufficient Input Validation vulnerability in NetScaler ADC and NetScaler Gateway.	No	No	False
CVE-2026-16723	Alibaba	Fastjson	Remote Code Execution vulnerability in Fastjson that allows unauthenticated remote attackers to execute arbitrary code on systems running vulnerable versions.	Yes	No	False
CVE-2026-18072	nico23	Advanced Responsive Video Embedder	Authentication Bypass vulnerability in Advanced Responsive Video	Yes	No	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
		for Rumble, Odysee, YouTube, Vimeo, Kick ... plugin for WordPress	Embedder for Rumble, Odysee, YouTube, Vimeo, Kick ... plugin for WordPress.			
CVE-2026-20896	Gitea	Docker Images	Authentication Bypass vulnerability in Gitea Docker Image versions allowing any source IP to impersonate a user when reverse-proxy authentication headers such as X-WEBAUTH USER are enabled.	No	No	True
CVE-2026-28496	FOSSBilling	FOSSBilling	Server-Side Template Injection vulnerability in FOSSBilling that can lead to information disclosure and remote code execution.	No	No	False
CVE-2026-29059	Windmill Labs	Windmill	Unauthenticated Path Traversal vulnerability in Windmill's get_log_file endpoint that enables an attacker to read arbitrary files on the server using ../ sequences.	No	No	False
CVE-2026-42897	Microsoft	Exchange Server	Cross-Site Scripting vulnerability in Microsoft Exchange Server in Outlook Web Access and when certain interaction conditions are met, arbitrary JavaScript can be executed in the browser context.	No	Yes	False
CVE-2025-2492	ASUS	AiCloud	Improper Authentication vulnerability in ASUS Router AiCloud that allows attackers to execute unauthorized functions via crafted requests.	No	Yes	False
CVE-2025-3248	Langflow	Langflow	Missing Authentication Vulnerability in Langflow in the */api/v1/validate/code* endpoint that allows a remote, unauthenticated attacker to execute arbitrary code via crafted HTTP requests.	No	Yes	True
CVE-2025-5777	Citrix	NetScaler ADC and Gateway	Out-of-Bounds Read vulnerability in Citrix	No	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			NetScaler ADC and Gateway due to insufficient input validation. This vulnerability can lead to memory overread when the NetScaler is configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server.			
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-2024-42009	Roundcube	Webmail	Cross-Site Scripting vulnerability in RoundCube Webmail that could allow a remote attacker to steal and send emails of a victim via a crafted e-mail message that abuses a Desanitization issue in *message_body()* in *program/actions/mail/show.php*.	No	Yes	True
CVE-2023-25717	Ruckus Wireless	Multiple Products	Cross-Site Request Forgery and Remote Code Execution vulnerability in multiple Ruckus Wireless Products in the web services component.	No	Yes	False
CVE-2021-29441	Alibaba	Nacos	Authentication Bypass in Alibaba Nacos platform that allows unauthenticated attackers to gain administrative access and perform any admin task on the Nacos Server, including configuration changes, service disruption, and data exposure.	No	Yes	True
CVE-2020-22653	Ruckus Wireless	Multiple Products	Improper Verification of Cryptographic Signature vulnerability in multiple Ruckus products.	No	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2020-22658	Ruckus Wireless	Multiple Products	Download of Code Without Integrity Check vulnerability in Multiple Ruckus Products	No	Yes	False

Ransomware Insights for July 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 July 2026	Targeted Industries	Vulnerabilities abused most
Qilin	The Qilin ransomware has been in existence since August 2022, also recognized as Agenda, 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.	124	• Manufacturing • Business Services • Technology • Healthcare • Construction	• CVE-2023-4966 • CVE-2023-20269 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-40044 • CVE-2022-36537 • CVE-2022-41082
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	104	• Manufacturing • Construction • Healthcare • Insurance • Consumer Services	• CVE-2025-7771 • CVE-2025-32433 • CVE-2025-33073 • CVE-2025-55182 • CVE-2024-55591

Ransomware	Description	No of affected organizations in July 2026	Targeted Industries	Vulnerabilities abused most
	related to backup, database, and security operations, maximizing operational disruption and impact.			
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.	41	• Manufacturing • Business Services • Technology • Healthcare • Construction	• CVE-2024-21412 • CVE-2024-21893 • CVE-2024-21887 • CVE-2024-57727 • CVE-2024-57728 • CVE-2024-57726 • CVE-2023-46805 • CVE-2021-44228
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	37	• Education • Healthcare • Government • Manufacturing • Information	• CVE-2025-4427 • CVE-2025-4428 • CVE-2025-5777 • CVE-2025-8088 • CVE-2025-10585

Ransomware	Description	No of affected organizations in July 2026	Targeted Industries	Vulnerabilities abused most
	algorithm, reinforcing its position as a structured and professionally run extortion operation.			
Safepay	SafePay ransomware is an emerging and previously undocumented threat, first observed in October 2024, that relies heavily on valid credentials likely sourced from dark web marketplaces and VPN access to infiltrate target environments. The group employs a multi-stage intrusion chain, commonly initiating attacks via Remote Desktop Protocol (RDP) and exploiting known VPN vulnerabilities while disabling defenses such as Windows Defender using LOLbins. SafePay features a modular and sophisticated design, enabling privilege escalation, UAC bypass, and network propagation, demonstrating a high degree of operational maturity. The ransomware encrypts files with a ***.safepay*** extension and drops a ***readme_safepay.txt*** ransom note, signaling the rise of a globally active ransomware operation targeting diverse industries across multiple countries.	28	• Manufacturing • Technology • Education • Healthcare • Business Services	• CVE-2025-8088 • CVE-2025-31324 • CVE-2025-53770 • CVE-2025-53771 • CVE-2025-61882
KRYBIT	KRYBIT is a sophisticated ransomware operation first observed in 2026 that encrypts files on compromised systems and appends the .KRYBIT extension, while dropping a ransom note named RECOVER-README.txt to initiate extortion procedures. The malware targeted documents, databases, archives, images, and enterprise-critical files, while simultaneously operating a double-extortion model that	25	• Business Services • Consumer Servies • Manufacturing • Technology • Public Sector	Unknown

Ransomware	Description	No of affected organizations in July 2026	Targeted Industries	Vulnerabilities abused most
	combined file encryption with theft of sensitive data including employee records, credentials, financial information, and technical design files. Victims were instructed to access multiple Tor-based onion communication portals hosted on Apache with PHP 8.0.30 using unique victim identifiers to negotiate recovery procedures and ransom payments. Observed operations affected at least 20 organizations across consumer services, business services, education, technology, and manufacturing sectors, with incidents identified in Germany, Mexico, Türkiye, Japan, and Austria.			
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.	22	• Manufacturing • Business Services • Technology • Construction • Agriculture	• CVE-2024-37085 • CVE-2024-40711 • CVE-2024-40766 • CVE-2023-20269 • CVE-2023-27532 • CVE-2023-28252 • CVE-2020-3259 • CVE-2020-3580

Ransomware	Description	No of affected organizations in July 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.	13	• Government • Education • Healthcare • Media • Information Technology	• CVE-2025-8088 • CVE-2025-29824 • CVE-2025-31161 • CVE-2025-31324 • CVE-2025-53770
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 communicate with the attacker via TOX messenger.	10	• Business Services • Manufacturing • Technology • Healthcare • Construction	Unknown
Payload	The Payload Ransomware is a lightweight C++ based ransomware (~385 KB) that operates without obfuscation, indicating prior attacker access and possible pre-disabling of AV/EDR defenses. The malware encrypts files using the ".payload" extension and drops a ransom note named RECOVER_payload.txt, leveraging a double-extortion model involving data exfiltration and Tor-based negotiation. It performs extensive pre-encryption actions, including deletion of shadow copies, clearing event logs, disabling security	6	• Manufacturing • Business Services • Hospitality • Healthcare • Financial Services	Unknown

Ransomware	Description	No of affected organizations in July 2026	Targeted Industries	Vulnerabilities abused most
	controls, and terminating backup and productivity services to maximize impact. The ransomware supports lateral movement via network share enumeration, uses multi-threaded execution, and employs ChaCha20 encryption with Curve25519 key exchange for efficiency and security. To evade detection and reduce forensic artifacts, it relaunches in hidden mode, leverages NTFS alternate data streams for self-deletion, and avoids encrypting critical system files to maintain operational stability.			

Conclusion

This month reaffirmed that the greatest risk to most organizations lay not in unknown threats, but in known vulnerabilities left unpatched long enough for attackers to reach them first. The convergence of rapid exploitation, expanding edge exposure, and relentless ransomware activity demonstrated that visibility and speed of remediation, rather than awareness alone, now separated resilient organizations from compromised ones. This is precisely the gap LOVI (Loginsoft Vulnerability Intelligence) is built to close, delivering early exploitation signals, prioritized remediation guidance, and threat-actor context that help defenders act before disclosure becomes breach. As adversaries continue to compress the window between discovery and attack, staying ahead of that curve remains the defining challenge of the months to come.