

Monthly Report

Threat & Vulnerabilities Report – September 2026

 CISCO

 citrix®

 MIKROTİK

 Microsoft

 Linux

 Google

 SONICWALL®

 JFrog

 CHECK POINT™

Executive Summary

September 2026 was the busiest month of the year for defenders. Patch queues grew faster than teams could clear them, attackers moved quickly from disclosure to weaponization, and ransomware operators kept up a steady stream of victim postings. CISA added 43 vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog during the month, the highest monthly total recorded in 2026. Cisco led with four additions, followed by Citrix, MikroTik, Microsoft, Linux, Google, and JFrog with three each, and SonicWall and Check Point with two each. The remaining entries covered a wide range of vendors, including Apple, Adobe, Arista, WordPress, Zyxel, ConnectWise, GitLab, and Fortinet. The spread showed that threat actors targeted network edge devices, enterprise software, developer tooling, and consumer platforms alike.

Active exploitation activity reflected the same breadth. Attackers went after AI and LLM infrastructure such as Langflow and BerriAI LiteLLM, which showed growing interest in the fast-expanding AI application stack. WordPress remained a favored target, with exploitation detected against the WebRehab Super Forms – Drag & Drop Form Builder and Elementor plugins. Threat actors also struck enterprise security and communication systems, exploiting Cisco Secure Firewall and Roundcube Webmail. Several of these campaigns hit flaws that already had patches available, which underscored how unpatched systems remained a dependable entry point for attackers.

Ransomware groups remained highly active throughout the month. TheGentlemen topped the leaderboard with 102 affected organizations, a substantial lead over Qilin, which claimed 74 victims. KRYBIT followed in third place with 34 organizations, while Safepay and IncRansom also contributed notable victim counts. The concentration of activity among a few prolific groups showed that established and emerging ransomware operations alike sustained aggressive campaigns, keeping extortion pressure on organizations across sectors.

Vulnerabilities added to the CISA KEV catalog in September 2026

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
CVE-2026-5430	WSO2	API Control Plane, API Manager, Traffic Manager, Universal Gateway	Path Traversal vulnerability in WSO2 API Control Plane, API Manager, Traffic Manager, and Universal Gateway that allows unrestricted file upload, leading to remote code execution.	No	No	False
CVE-2026-7273	Zyxel	GS1900 Series Switches	Stack-Based Buffer Overflow vulnerability in the CGI program of Zyxel GS1900 Series Switches that allows a LAN-based, unauthenticated	No	No	False

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
			attacker to execute OS commands via a crafted HTTP request.			
<u>CVE-2026-9586</u>	Sangoma	Switchvox	SQL Injection vulnerability in Sangoma Switchvox that allows an unauthenticated remote attacker to execute arbitrary SQL statements against the backend PostgreSQL database with a single crafted request, leading to database manipulation and remote code execution.	No	No	False
<u>CVE-2026-19490</u>	Citrix	NetScaler ADC and NetScaler Gateway	Authentication Bypass Using an Alternate Path or Channel vulnerability in Citrix NetScaler ADC and NetScaler Gateway that allows an unauthenticated remote attacker to bypass authentication when the appliance is configured as an AAA virtual server or as a Gateway (SSL VPN, ICA Proxy, CVPN, or RDP Proxy).	No	No	False
<u>CVE-2026-20079</u>	Cisco	Secure Firewall Management Center (FMC) and Security Cloud Control (SCC) Firewall Management	Authentication Bypass Using an Alternate Path or Channel vulnerability in Cisco Secure Firewall Management Center (FMC) and Security Cloud Control (SCC) Firewall Management that allows an unauthenticated remote attacker to bypass authentication and execute script files to obtain root access to the underlying operating system.	No	<u>Yes</u>	False
<u>CVE-2026-42016</u>	JFrog	Artifactory	Incorrect Authorization vulnerability in JFrog Artifactory that allows privilege escalation because token validation checks the signature and issuer but not the scope of the token.	No	No	False
<u>CVE-2026-42018</u>	JFrog	Artifactory	Improper Authentication vulnerability in JFrog	No	No	False

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
			Artifactory that can return an internal anonymous-user token to an unauthenticated caller when anonymous access is disabled, potentially exposing sensitive resources.			
<u>CVE-2026-48710</u>	Kludex	Starlette	HTTP Request/Response Smuggling vulnerability in Kludex Starlette that allows attackers to inject paths into the host part of a request, prepending the actual path and leading to authentication bypass when authentication depends on the reconstructed URL path. This vulnerability can be chained with CVE-2026-42271.	No	No	True
<u>CVE-2026-49869</u>	Kestra	Kestra OSS	OS Command Injection vulnerability in Kestra OSS that allows an unauthenticated remote attacker to create and execute arbitrary workflows without credentials.	No	No	False
<u>CVE-2026-53266</u>	Linux	Kernel	Out-of-Bounds Write vulnerability in the Linux Kernel ebttables SNAT target that allows an ARP sender hardware address rewrite to write directly into a nonlinear socket-buffer fragment backed by a splice-imported file page. Impacted products could be end-of-life (EoL) or end-of-service (EoS).	No	No	True
<u>CVE-2026-58704</u>	Google	Pixel	Improper Authorization vulnerability in the cellular modem of Google Pixel devices, where a logic error allows an attacker to bypass permission checks and escalate privileges.	<u>Yes</u>	No	True
<u>CVE-2026-59822</u>	BerriAI	LiteLLM	Improper Authentication vulnerability in the MCP Streamable HTTP endpoint of BerriAI LiteLLM that allows	No	No	True

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
			an unauthenticated attacker to establish an authenticated MCP session using an arbitrary Bearer token.			
<u>CVE-2026-65660</u>	Microsoft	SharePoint	Code Injection vulnerability in Microsoft SharePoint that allows an authorized attacker to execute code over a network.	No	No	False
<u>CVE-2026-67277</u>	MikroTik	RouterOS	Missing Authentication for Critical Function vulnerability in the btest service of MikroTik RouterOS that allows kernel memory disclosure and denial of service.	<u>Yes</u>	No	False
<u>CVE-2026-67279</u>	MikroTik	RouterOS	Improper Enforcement of Behavioral Workflow vulnerability in MikroTik RouterOS that allows an unauthenticated client to open a session channel and send an exec request. This vulnerability can be chained with CVE-2026-86060 for unauthenticated exploitation.	<u>Yes</u>	No	True
<u>CVE-2026-71362</u>	Adobe	Commerce and Magento	Incorrect Authorization vulnerability in Adobe Commerce and Magento that allows an attacker to gain elevated access to sensitive resources without any user interaction.	No	No	False
<u>CVE-2026-75650</u>	Adobe	Commerce and Magento Open Source	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Adobe Commerce and Magento Open Source that allows an attacker to execute arbitrary code.	<u>Yes</u>	No	False
<u>CVE-2026-76460</u>	Cisco	Identity Services Engine (ISE) and ISE Passive Identity Connector (ISE-PIC)	Incorrect Use of Privileged APIs vulnerability in Cisco Identity Services Engine (ISE) and ISE Passive Identity Connector (ISE-PIC) that allows an unauthenticated	<u>Yes</u>	No	False

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
			remote attacker to gain unauthorized access to the affected device by bypassing the web-based management interface.			
<u>CVE-2026-76461</u>	Cisco	Secure Email Gateway (SEG)	SQL Injection vulnerability in Cisco AsyncOS Software for Cisco Secure Email Gateway (SEG) that allows an unauthenticated remote attacker to execute arbitrary commands with root privileges on the underlying operating system.	<u>Yes</u>	No	False
<u>CVE-2026-76504</u>	Cisco	Catalyst SD-WAN Manager	Hex Encoding vulnerability in Cisco Catalyst SD-WAN Manager that could allow an unauthenticated, remote attacker to access an affected system with privileges of the admin user due to improper handling of URI encoding in an HTTP request.	<u>Yes</u>	No	False
<u>CVE-2026-81963</u>	Microsoft	Windows	Link Following vulnerability in the Microsoft Windows Update Stack that allows a local attacker to escalate privileges up to SYSTEM.	<u>Yes</u>	No	False
<u>CVE-2026-82329</u>	JFrog	Artifactory	Improper Authentication vulnerability in JFrog Artifactory that, under default configuration, allows an unauthenticated attacker with network access to obtain administrative privileges.	No	No	False
<u>CVE-2026-83548</u>	SonicWall	SMA1000 Appliances	Server-Side Request Forgery vulnerability in SonicWall SMA1000 Appliances that allows a remote unauthenticated attacker to gain unauthorized access to sensitive functionality and perform unauthorized operations.	<u>Yes</u>	No	False
<u>CVE-2026-83549</u>	SonicWall	SMA1000 Appliances	OS Command Injection vulnerability in SonicWall SMA1000 Appliances that	<u>Yes</u>	No	False

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
			allows a remote authenticated attacker with administrator privileges to execute arbitrary OS commands, resulting in remote code execution.			
<u>CVE-2026-84869</u>	ConnectWise	ScreenConnect	Improper Privilege Management and Missing Authorization vulnerability in ConnectWise ScreenConnect that allows an attacker to transfer and execute files through an active remote session without authorization or host confirmation.	<u>Yes</u>	No	False
<u>CVE-2026-85046</u>	Google	Chromium V8	Type Confusion vulnerability in Google Chromium V8 that allows a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. This vulnerability can impact multiple Chromium-based browsers, including Google Chrome, Microsoft Edge, and Opera.	<u>Yes</u>	<u>Yes</u>	True
<u>CVE-2026-85102</u>	Check Point	Security Gateway and Spark Firewall	Improper Certificate Validation vulnerability in Check Point Security Gateway and Spark Firewall using Site to Site VPN or Remote Access VPN that allows an unauthenticated remote attacker to execute arbitrary code on the Gateway.	No	No	False
<u>CVE-2026-85706</u>	GitLab	Community Edition (CE) and Enterprise Edition (EE)	Path Traversal vulnerability in the repository commits API of GitLab Community Edition and Enterprise Edition that allows an unauthenticated user to read arbitrary files due to improper path confinement and missing authentication enforcement.	No	No	True
<u>CVE-2026-85880</u>	Microsoft	Windows	Heap-Based Buffer Overflow vulnerability in Microsoft Windows Advanced Local	<u>Yes</u>	<u>Yes</u>	False

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
			Procedure Call (ALPC) that allows an attacker to elevate privileges locally.			
<u>CVE-2026-86060</u>	MikroTik	RouterOS	Improper Neutralization of Argument Delimiters in a Command vulnerability in MikroTik RouterOS that allows an attacker to change the trusted RouterOS policy mask, leading to privilege escalation.	<u>Yes</u>	No	False
<u>CVE-2026-86218</u>	N-able	N-central	Static Code Injection vulnerability in N-able N-central that allows for pre-authentication remote code execution.	<u>Yes</u>	No	False
<u>CVE-2026-86950</u>	Apple	Multiple Products	Out-of-Bounds Write vulnerability in Apple Multiple Products in CoreGraphics that may lead to arbitrary code execution.	<u>Yes</u>	No	False
<u>CVE-2026-87491</u>	Google	Chromium V8	Out-of-Bounds Write vulnerability in Google Chromium V8 that allows a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. This vulnerability can impact multiple Chromium-based browsers, including Google Chrome, Microsoft Edge, and Opera.	<u>Yes</u>	<u>Yes</u>	True
<u>CVE-2026-87886</u>	Acronis	Backup plugin for cPanel & WHM and extension for Plesk	Incorrect Default Permissions vulnerability in the Acronis Backup plugin for cPanel & WHM and extension for Plesk that allows for privilege escalation.	No	No	False
<u>CVE-2026-87902</u>	WordPress	Core	Remote File Inclusion vulnerability in WordPress Core that allows an unauthenticated attacker to force page-template resolution to include a chosen readable local .php file outside the active theme directories, leading to remote code execution.	No	No	True

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
<u>CVE-2026-88771</u>	Citrix	NetScaler	Improper Input Validation vulnerability in Citrix NetScaler that could allow an unauthenticated attacker to execute arbitrary commands.	<u>Yes</u>	No	False
<u>CVE-2026-88772</u>	Citrix	NetScaler	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in Citrix NetScaler that could allow for remote code execution or denial of service.	<u>Yes</u>	No	False
<u>CVE-2026-93616</u>	Check Point	Security Management Server, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, SmartEvent	Path Traversal vulnerability in Check Point Security Management Server, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, and SmartEvent that allows an unauthenticated attacker to upload and execute arbitrary scripts.	<u>Yes</u>	No	False
<u>CVE-2026-93952</u>	Arista	VeloCloud Orchestrator (VCO)	Improper Input Validation vulnerability in on-premises Arista VeloCloud Orchestrator (VCO) that allows a remote attacker to access privileged internal functionality, compromising the confidentiality, integrity, and availability of the orchestrator and the data it manages.	<u>Yes</u>	No	False
<u>CVE-2026-94127</u>	F5	BIG-IP APM	Heap-Based Buffer Overflow vulnerability in F5 BIG-IP APM that allows an unauthenticated attacker to achieve remote code execution when an access policy and an OAuth profile are configured on a virtual server.	<u>Yes</u>	No	False
<u>CVE-2025-25249</u>	Fortinet	FortiOS, FortiSwitchManager, FortiSASE	Heap-Based Buffer Overflow vulnerability in Fortinet FortiOS, FortiSwitchManager, and FortiSASE that allows an attacker to execute	No	<u>Yes</u>	False

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
			unauthorized code or commands via specially crafted packets.			
CVE-2025-39682	Linux	Kernel	Improper Check for Unusual or Exceptional Conditions vulnerability in the Linux Kernel TLS receive path that allows a zero-length record retrieved from rx_list to bypass the intended recvmsg() record-type handling, causing subsequent TLS records to be processed under incorrect zero-copy and queuing assumptions. Impacted products could be end-of-life (EoL) or end-of-service (EoS).	No	No	True
CVE-2025-39964	Linux	Kernel	Race Condition vulnerability in the Linux Kernel that allows concurrent writes to the same AF_ALG socket, causing data to be unpredictably interleaved and creating inconsistencies in the internal state of the socket.	No	No	True

Actively Exploited Vulnerabilities in September 2026

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-0768	Langflow	Langflow	Remote Code Execution vulnerability in Langflow that allows remote attackers to execute arbitrary code on affected installations.	Yes	No	False
CVE-2026-14894	WebRehab	Super Forms - Drag & Drop Form Builder	Unrestricted Arbitrary File Upload vulnerability in the Super Forms -Drag & Drop Form Builder plugin for WordPress made it possible for unauthenticated attackers to upload files that may be executable,	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			making remote code execution possible.			
<u>CVE-2026-20316</u>	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	<u>Yes</u>	<u>Yes</u>	False
<u>CVE-2026-27540</u>	Rymera Web Co Pty Ltd	Woocommerce Wholesale Lead Capture	Unrestricted Upload of File with Dangerous Type vulnerability in Rymera Web Co Pty Ltd. Woocommerce Wholesale Lead Capture plugin	No	No	False
<u>CVE-2026-32475</u>	Elementor	Elementor Pro plugin for WordPress	Unrestricted Upload of File with Dangerous Type vulnerability in Elementor Pro plugin for WordPress that can be leveraged by unauthenticated attackers to upload arbitrary files, including executable PHP files, to a vulnerable site, which can lead to remote code execution and complete site takeover.	No	No	False
<u>CVE-2026-35029</u>	BerriAI	LiteLLM	An Authorization Bypass vulnerability in LiteLLM proxy server allowing authenticated users to modify proxy configurations and environment variables.	No	No	True
<u>CVE-2026-39364</u>	vitejs	vite	Information Disclosure via Path Traversal vulnerability in Vite MinimOS that allows remote unauthenticated attackers to steal cloud credentials and configurations from AWS and Azure deployments.	No	No	True
<u>CVE-2026-48842</u>	Roundcube	Webmail	Pre-Authentication SQL Injection vulnerability in Roundcube Webmail that	No	No	True

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			allows an attacker to send specially crafted input to manipulate a database query before successfully logging in to the webmail application.			
<u>CVE-2026-58138</u>	conductor-oss	conductor	Unauthenticated Remote Code Execution vulnerability in Orkes Conductor that allows remote attackers to execute arbitrary OS commands by submitting inline workflow definitions containing malicious JavaScript or Python expressions to the workflow API endpoint prior to authentication.	No	No	False
<u>CVE-2026-60004</u>	Gitea	Gitea	Code Injection vulnerability in Gitea that allows an attacker with repository write access to send a malicious patch to the diffpatch API endpoint to plant an executable Git hook and run shell commands as the Gitea service account	No	<u>Yes</u>	True
<u>CVE-2026-66066</u>	Ruby on Rails	Rails	Arbitrary File Read and Remote Code Execution in Active Storage component of Ruby on Rails	No	No	True
<u>CVE-2026-67276</u>	MikroTik	RouterOS	Improper Verification of Cryptographic Signature vulnerability in MikroTik RouterOS caused by incomplete validation of RSA public keys.	<u>Yes</u>	No	False
<u>CVE-2026-78006</u>	stellarwp	The Events Calendar	Remote Code Execution vulnerability in the Events Calendar plugin for WordPress via the <i>is_safe_widget_instance</i> function.	No	No	False
<u>CVE-2026-89026</u>	Issabel Foundation	Issabel Framework	Use of Hard-Coded Cryptographic Key vulnerability in Issabel Framework that allows unauthenticated remote	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			attackers to forge valid bearer tokens.			
CVE-2026-100382	Wikimedia Foundation	Mediawiki - ExternalData Extension	OS Command Injection vulnerability in Wikimedia Foundation Mediawiki - ExternalData Extension	No	No	False

Ransomware Insights for September 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 September 2026	Targeted Industries	Vulnerabilities abused most
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.	102	• Manufacturing • Construction • Healthcare • Insurance • Consumer Services	• CVE-2025-7771 • CVE-2025-32433 • CVE-2025-33073 • CVE-2025-55182 • CVE-2024-55591
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 <i>Ransom.Win32.AGENDA.THIAFBB</i> , 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.	74	• 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

Ransomware	Description	No of affected organizations in September 2026	Targeted Industries	Vulnerabilities abused most
<u>KRYBIT</u>	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 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.	34	• Business Services • Consumer Servies • Manufacturing • Technology • Public Sector	Unknown
<u>Safepay</u>	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,	29	• Manufacturing • Technology • Education • Healthcare • Business Services	• CVE-2025-8088 • CVE-2025-31324 • CVE-2025-53770 • CVE-2025-53771 • CVE-2025-61882

Ransomware	Description	No of affected organizations in September 2026	Targeted Industries	Vulnerabilities abused most
	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.			
<u>IncRansom</u>	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.	28	• Education • Healthcare • Government • Manufacturing • Information	• CVE-2025-4427 • CVE-2025-4428 • CVE-2025-5777 • CVE-2025-8088 • CVE-2025-10585
<u>Akira</u>	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,	27	• 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 September 2026	Targeted Industries	Vulnerabilities abused most
	combined with data exfiltration via tools like rclone and SCP, makes Akira particularly effective against modern, virtualization-heavy networks.			
<u>Clop</u>	CLOP ransomware, first observed in 2019, is known for its advanced techniques and aggressive targeting of large enterprises. Initially, the ransomware group relied on phishing emails and remote desktop protocol (RDP) exploits to gain initial access to victims' networks. Once inside, CLOP would spread laterally, encrypting critical data and demanding a ransom payment for decryption.	25	• Healthcare • Bank • Education • Gaming • Transportation	• CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-47246
<u>Lockbit5</u>	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.	15	• Business Services • Manufacturing • Technology • Healthcare • Construction	• Unknown
<u>Play</u>	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.	11	• Government • Education • Healthcare • Media • Information Technology	• CVE-2025-8088 • CVE-2025-29824 • CVE-2025-31161 • CVE-2025-31324 • CVE-2025-53770
<u>Dragonforce</u>	DragonForce is a ransomware group originating from Malaysia. Initially, known as a hacktivist group, DragonForce has transitioned into a ransomware	10	• Manufacturing • Business Services • Technology • Healthcare	• CVE-2024-21412 • CVE-2024-21893 • CVE-2024-21887 • CVE-2024-57727 • CVE-2024-57728

Ransomware	Description	No of affected organizations in September 2026	Targeted Industries	Vulnerabilities abused most
	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.		• Construction	• CVE-2024-57726 • CVE-2023-46805 • CVE-2021-44228

Conclusion

September 2026 showed how short the window between disclosure and exploitation had become, as threat actors weaponized flaws across edge devices, AI platforms, and widely used web applications. Record KEV additions, persistent targeting of unpatched systems, and sustained ransomware activity left little room for delayed remediation. Organizations that prioritized patching by real-world exploitation, rather than severity scores alone, stood in the strongest position to reduce their exposure. LOVI (Loginsoft Vulnerability Intelligence) can help security teams stay ahead of these threats with timely, actionable insight into the vulnerabilities that matter most, so they can prioritize remediation with confidence.



Connect with us

 [linkedin.com/loginsoft](https://www.linkedin.com/loginsoft)

 x.com/loginsoft_inc

 www.loginsoft.com

