loginsoft

Monthly Report

Threat & Vulnerabilities Report – August 2026

Executive Summary

August 2026 proved a relentless month for defenders, as CISA added 32 vulnerabilities to its Known Exploited Vulnerabilities catalog, confirming that attackers were actively breaking into real systems across a wide sweep of enterprise technology. Microsoft led the additions with five flaws, followed by two apiece from PaperCut NG/MF, N-able N-central, TrueConf, and Red Hat, with single entries spanning IBM, Apache, N-able, JetBrains, Progress, Metabase, Cisco, Ray Project, Apple, Broadcom, MLflow, Synacor, Oracle, Gitea, Citrix, Ajax.NET Professional, ownCloud, and JFrog. The catalog additions reached from operating systems and virtualization platforms to print management, artifact repositories, AI tooling, and decade-old open-source components, underscoring how attackers weaponized both freshly disclosed flaws and long-forgotten ones with equal ease.

Beyond the catalog, active exploitation struck platforms including Palo Alto Networks, BeyondTrust, and Citrix, several within days of disclosure. The month also spotlighted determined state-aligned and financially motivated actors: the China-linked QTFY group breached US critical infrastructure using its custom scanning and botnet platforms, the Chinese-speaking UAT-10147 group deployed the cross-platform SPECTRE backdoor while folding AI into its operations, and the Mirai-derived Evooo1Bot botnet turned internet-facing edge devices into stealthy proxy relays and attack nodes.

Ransomware pressure intensified in parallel, with Qilin topping the month at 162 affected organizations, followed by TheGentlemen with 111 and Cl0p with 85.

Vulnerabilities added to the CISA KEV catalog in August 2026

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-8037	Progress	LoadMaster	Command Injection vulnerability in Progress LoadMaster that allows an un-authenticated attacker to execute arbitrary commands on the LoadMaster appliance by exploiting unsanitized input in multiple command endpoints.	No	No	False
CVE-2026-8452	Citrix	NetScaler ADC and NetScaler Gateway	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in Citrix NetScaler ADC and NetScaler Gateway which could lead to denial of service.	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-9198	IBM	Langflow	Code Injection Vulnerability in IBM Langflow that allows unauthenticated attackers to achieve full remote code execution on default Langflow deployments.	No	No	False
CVE-2026-18556	N-able	N-central	Authentication Bypass Using an Alternate Path or Channel vulnerability in N-able N-central that allows for authentication bypass.	No	No	False
CVE-2026-18577	N-able	N-central	Authentication Bypass Using an Alternate Path or Channel vulnerability in N-able N-central allows for authentication bypass and account takeover in N-central. This vulnerability is the result of an incomplete patch for CVE-2026-18556.	No	No	False
CVE-2026-20349	Cisco	Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD)	Heap Inspection vulnerability in Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) that could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	Yes	No	False
CVE-2026-21962	Oracle	HTTP Server and Oracle Weblogic Server Proxy Plug-in	Improper Access Control vulnerability in Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in that can result in unauthorized creation, deletion or modification access to critical data as well as unauthorized access to critical data or complete access to all Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in accessible data.	No	No	False
CVE-2026-33824	Microsoft	Internet Key Exchange (IKE) Service Extensions	Double Free vulnerability in Microsoft Internet Key Exchange (IKE) Service Extensions that enable remote code execution.	No	Yes	False
CVE-2026-34486	Apache	Tomcat	Missing Encryption of Sensitive Data vulnerability in	No	No	True

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			Apache Tomcat that allows the bypass of the *EncryptInterceptor*. This vulnerability can be chained with CVE-2025-24813.			
CVE-2026-53362	Linux	Kernel	Out-of-Bounds Write vulnerability in Linux Kernel that can allow for privilege escalation via IPv6 networking subsystem. This vulnerability can impact multiple products, including but not limited to Suse, Red Hat, and other products using Linux.	No	No	True
CVE-2026-55040	Microsoft	SharePoint	Weak Authentication vulnerability in Microsoft SharePoint that allows an unauthorized attacker to bypass a security feature over a network.	No	No	False
CVE-2026-59310	Broadcom	VMware vCenter	Path Traversal vulnerability in Broadcom VMware vCenter that could allow a threat actor with network access to vCenter to execute arbitrary code.	No	No	False
CVE-2026-60004	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	No	True
CVE-2026-63077	JetBrains	TeamCity	Deserialization of Untrusted Data vulnerability in JetBrains TeamCity that could allow unauthenticated remote code execution via the agent polling protocol.	No	No	False
CVE-2026-64849	MLflow	MLflow	Server-Side Request Forgery vulnerability in MLflow that allows attackers to reach internal or cloud metadata services and receive ***response_status*** and ***response_body***.	No	No	True
CVE-2026-65400	Apple	macOS	Improper Authentication vulnerability in Apple macOS that could allow an attacker on the network to	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			authenticate to Screen Sharing without valid credentials.			
CVE-2026-66384	JFrog	Artifactory	Improper Limitation of a Pathname to a Restricted Directory vulnerability in JFrog Artifactory that can allow an authenticated user to write data outside the intended Docker cache path under specific remote-repository conditions.	Yes	No	False
CVE-2026-68820	Microsoft	Windows	Use-After-Free vulnerability in Microsoft Windows Ancillary Function Driver for WinSock that allows an authorized attacker to elevate privileges locally.	Yes	Yes	False
CVE-2026-72529	TrueConf	Server	Missing Authentication for Critical Function vulnerability in TrueConf Server which could allow a remote unauthorized attacker with network access via port 4307/TCP to execute an arbitrary script.	No	Yes	False
CVE-2026-72530	TrueConf	Server	Code Injection vulnerability in TrueConf Server that could allow an unauthorized remote attacker with network access via port 4307/TCP to use a specially crafted script to break out of the isolated environment and execute arbitrary code on the host system.	No	Yes	False
CVE-2026-72898	Metabase	Metabase	SQL Injection vulnerability in Metabase that allows an unauthenticated remote attacker to inject arbitrary SQL into the Metabase application database, which can give them administrator access to the instance. From there, the attacker could change the application configuration, steal stored credentials for the connected databases, read any data accessible through those connections, and export data.	Yes	No	True

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-73570	Synacor	Zimbra Collaboration Suite (ZCS)	OS Command Injection vulnerability in Zimbra Collaboration Suite (ZCS) which could allow an unauthenticated attacker to send specially crafted SMTP requests that may result in execution of arbitrary operating system commands as the Zimbra user.	No	No	False
CVE-2026-81578	PaperCut	NG/MF	Missing Authentication for Critical Function vulnerability in PaperCut NG/MF which allows an unauthenticated remote attacker to modify certain system configurations. This vulnerability can be chained with CVE-2026-82078.	Yes	No	False
CVE-2026-82078	PaperCut	NG/MF	Unsafe Reflection vulnerability in PaperCut NG/MF that allows an attacker to manipulate system configuration parameters and execute arbitrary Java bytecode residing on the application classpath under the security context of the PaperCut server process. This vulnerability can be chained with CVE-2026-81578.	Yes	No	False
CVE-2025-62593	Ray-Project	Ray	Code Injection vulnerability in Ray-Project Ray that allow remote code execution. Developers using Ray as a development tool may be exposed to this vulnerability exploitable through Firefox and Safari.	Yes	Yes	True
CVE-2023-49105	ownCloud	ownCloud	Improper Authentication vulnerability in ownCloud that allows an attacker to access, modify, or delete any file without authentication if the username of a victim is known, and the victim has no signing-key configured.	No	No	False
CVE-2022-0995	Linux	Kernel	Out-of-Bounds Write vulnerability in Linux Kernel which could allow a local user to gain privileged access or	No	Yes	True

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			cause a denial of service on the system.			
CVE-2021-23758	Ajax.NET Professional	Ajax.NET Professional	Deserialization of Untrusted Data vulnerability in Ajax.NET Professional that could allow for remote code execution via arbitrary .NET classes.	No	Yes	True
CVE-2019-1068	Microsoft	SQL Server	Remote Code Execution vulnerability in Microsoft SQL Server that could allow an attacker to execute code in the context of the SQL Server Database Engine service account.	No	Yes	False
CVE-2015-3246	Red Hat	Libuser	Race Condition vulnerability in Red Hat Libuser that allows authenticated local users to corrupt the /etc/passwd file to cause a denial of service or privilege escalation.	No	Yes	True
CVE-2015-5287	Red Hat	Automatic Bug Reporting Tool	Privilege Escalation vulnerability in Red Hat Automatic Bug Reporting Tool that could allow local users with certain permissions to gain privileges via a symlink attack on a file with a predictable name.	No	Yes	True

Actively Exploited Vulnerabilities in August 2026

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-0300	Palo Alto Networks	PAN-OS	Out-of-bounds Write vulnerability in Palo Alto Networks PAN-OS	No	Yes	False
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).	Yes	Yes	False
CVE-2026-3055	Citrix	NetScaler	Out-of-Bounds Read vulnerability in Citrix NetScaler ADC, Gateway, and NetScaler ADC FIPS and NDcPP when configured as a SAML IDP leading to memory overread.	No	Yes	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 appliance 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-2026-15826	Cozmoslabs	The User Profile Builder plugin for WordPress	Unauthenticated Authentication Bypass via Type Confusion vulnerability in The User Profile Builder plugin for WordPress that can lead to account takeover.	No	No	False
CVE-2026-15981	miniOrange	miniOrange SAML 2.0 Single Sign-On (SSO) plugin for WordPress	Authentication Bypass vulnerability in miniOrange SAML 2.0 Single Sign-On WordPress plugin that makes it possible for an attacker to sign in as any WordPress user, including administrators.	No	No	False
CVE-2026-19478	GitLab	• Community Edition (CE) • Enterprise Edition (EE)	Code Injection vulnerability in the GitLab Community Edition and Enterprise Edition software that, under certain conditions, could allow an unauthenticated attacker to remotely modify or delete public projects and user data.	No	No	True
CVE-2026-19632	Cozmoslabs	Translate Multilingual sites with AI Translation plugin for WordPress	Unauthenticated Account Takeover via Password Reset Link Disclosure vulnerability in the TranslatePress - Translate Multilingual sites with AI Translation plugin for WordPress that enables full administrator account takeover.	No	No	False
CVE-2026-21858	n8n	n8n	Improper Input Validation vulnerability in n8n	No	Yes	True

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-33017	Langflow	Langflow	Code Injection vulnerability in Langflow that could allow building public flows without requiring authentication.	No	Yes	True
CVE-2026-39987	Marimo	Marimo	Remote Code Execution vulnerability in Marimo allowing an unauthenticated attacker to shell access and execute arbitrary system commands.	No	Yes	True
CVE-2026-58231	SAP	SAP Commerce Cloud	Improper Authorization and Input Validation vulnerability in SAP Commerce Cloud that allows an unauthenticated attacker to abuse a default authentication client and submit specially crafted input to certain functions lacking sufficient validation.	No	No	False
CVE-2026-61979	miniOrange	miniOrange SAML 2.0 Single Sign-On (SSO) plugin for WordPress	Unauthenticated Privilege Escalation vulnerability in the SAML SP Sign-On WordPress plugin by miniOrange that makes it possible for an attacker to sign in as any WordPress user, including administrators.	No	No	False
CVE-2026-69836	Microsoft	Entra ID	Deserialization of Untrusted Data vulnerability in Microsoft Entra ID that allows an unauthorized attacker to execute a code over a network.	No	No	False
CVE-2026-71362	Adobe	Commerce and Magento	Incorrect Authorization vulnerability in Adobe Commerce and Magento e-commerce platforms that could be leveraged to gain elevated access to sensitive resources.	No	No	False
CVE-2026-71479	QuantumNous	New API	Integer Overflow vulnerability in the New API that lets a user with a small balance credit themselves an enormous one.	No	No	True
CVE-2026-77136	in2code	powermail	Server-Side Template Injection vulnerability in the "powermail" extension for TYPO3 CMS, that enables an unauthenticated attacker to	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			inject and execute malicious commands remotely.			
CVE-2026-77647	SPIP	SPIP	Unauthenticated Remote Code Execution vulnerability in SPIP CMS.	No	No	False
CVE-2026-77806	SPIP	SPIP	Code Injection vulnerability in SPIP content management system that allows unauthenticated remote attackers to execute arbitrary code.	No	No	False
CVE-2025-24472	Fortinet	FortiOS and FortiProxy	Authentication Bypass vulnerability in Fortinet FortiOS and FortiProxy that allows a remote attacker to gain super-admin privileges via crafted CSF proxy requests.	No	Yes	False
CVE-2025-31161	CrushFTP	CrushFTP	Authentication Bypass vulnerability in CrushFTP.	Yes	Yes	False
CVE-2024-8190	Ivanti	Cloud Services Appliance	OS Command Injection vulnerability in Ivanti Cloud Services Appliance.	No	Yes	False
CVE-2024-8963	Ivanti	Cloud Services Appliance	Path Traversal vulnerability in Ivanti Cloud Services Appliance.	No	Yes	False
CVE-2024-9380	Ivanti	Cloud Services Appliance	OS Command Injection vulnerability in Ivanti Cloud Services Appliance.	No	Yes	False
CVE-2024-24919	Check Point	Quantum Security Gateways	Information Disclosure vulnerability in Check Point Quantum Security Gateways.	No	Yes	False
CVE-2024-29269	Telesquare	TLR-2005Ksh	Command Injection vulnerability in Telesquare TLR-2005Ksh 1.0.0 and 1.1.4	No	Yes	False
CVE-2023-22515	Atlassian	Confluence Data Center and Server	Broken Access Control vulnerability in Atlassian Confluence Data Center and Server.	No	Yes	False
CVE-2022-0847	Linux	Kernel	Privilege Escalation vulnerability in Linux Kernel where an unprivileged local user could escalate their privileges on the system.	No	Yes	True
CVE-2022-0995	Linux	Kernel	Out-of-Bounds Write vulnerability in Linux Kernel which could allow a local user to gain privileged access or cause a denial of service on the system.	No	Yes	True

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2022-27925	Synacor	Zimbra Collaboration Suite (ZCS)	Arbitrary File Upload vulnerability in Synacor Zimbra Collaboration Suite in the *mboximport* functionality, allowing an authenticated attacker to upload arbitrary files to perform remote code execution.	No	Yes	False
CVE-2022-37055	D-Link	Routers	Buffer Overflow vulnerability in D-Link Routers that has a high impact on confidentiality, integrity, and availability.	No	Yes	False
CVE-2021-3156	Sudo	Sudo	Heap-Based Buffer Overflow vulnerability in Sudo which allows for privilege escalation.	No	Yes	True
CVE-2020-10987	Tenda	AC1900 Router AC15 Model	Remote Code Execution vulnerability in Tenda AC1900 Router AC15 Model.	No	Yes	False

Ransomware Insights for August 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 August 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.	162	• 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	111	• Manufacturing • Construction • Healthcare	• CVE-2025-7771 • CVE-2025-32433 • CVE-2025-33073

Ransomware	Description	No of affected organizations in August 2026	Targeted Industries	Vulnerabilities abused most
	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.		• Insurance • Consumer Services	• CVE-2025-55182 • CVE-2024-55591
Cl0p	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.	85	• Healthcare • Bank • Education • Gaming • Transportation	• CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-47246
IncRansom	INC is a ransomware-as-a-service (RaaS) operation that emerged in mid-to-late 2023, operating through an affiliate-driven model in which core operators supply the malware and infrastructure while affiliates conduct intrusions and share profits. The group relies on a double-extortion strategy, coercing victims by threatening data leaks under the pretext of "protecting their reputation." INC maintains two dedicated leak sites a private, credential-protected portal used for victim communication and negotiation, and a public site used to release stolen data. First detected in July 2023 and tracked by Trend Micro as Water Anito, the ransomware encrypts files using AES algorithm, reinforcing its position as a structured and professionally run extortion operation.	38	• Education • Healthcare • Government • Manufacturing • Information	• CVE-2025-4427 • CVE-2025-4428 • CVE-2025-5777 • CVE-2025-8088 • CVE-2025-10585
KRYBIT	KRYBIT is a sophisticated ransomware operation first observed in 2026 that encrypts files on compromised systems and appends	36	• Business Services	Unknown

Ransomware	Description	No of affected organizations in August 2026	Targeted Industries	Vulnerabilities abused most
	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.		• Consumer Servies • Manufacturing • Technology • Public Sector	
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.	20	• 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
Play	Play ransomware was first seen in June 2022, targeting organizations through various initial access methods, such as exploiting vulnerabilities in Remote Desktop	16	• Government • Education • Healthcare • Media	• CVE-2025-8088 • CVE-2025-29824 • CVE-2025-31161 • CVE-2025-31324

Ransomware	Description	No of affected organizations in August 2026	Targeted Industries	Vulnerabilities abused most
	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.		• Information Technology	• 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.	15	• Business Services • Manufacturing • Technology • Healthcare • Construction	Unknown
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.	14	• 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
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.	11	• 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 August 2026	Targeted Industries	Vulnerabilities abused most
	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.			

Conclusion

August 2026 stood out as one of the most critical and active months of the year, both in the sheer volume of CISA KEV additions and in the pace of confirmed active exploitation across enterprise, open-source, and AI infrastructure. The convergence of state-aligned campaigns, aggressive botnets, and record ransomware activity made clear that attackers moved faster than ever, leaving little room between disclosure and compromise. Organizations that patched promptly, hardened internet-facing systems, and monitored for exploitation stood the best chance of staying ahead. Loginsoft Vulnerability Intelligence (LOVI) tracks these developments as they unfold, delivering the timely, source-anchored intelligence organizations need to act before threats reach their doors.