loginsoft

Monthly Report

Threat & Vulnerabilities Report – October 2026



Executive Summary

October marked Cybersecurity Awareness Month, yet threat actors treated the month as an open invitation rather than a warning. Defenders faced a steady stream of newly weaponized flaws, a crowded CISA KEV catalog, and ransomware operations that showed no sign of slowing. The month underscored a simple truth: awareness alone did not close the gap between disclosure and exploitation.

CISA added 36 vulnerabilities to the Known Exploited Vulnerabilities (KEV) catalog in October, confirming real-world exploitation across a wide spread of enterprise and consumer technologies. Plex led the vendor tally with four additions, while Ivanti, Cisco, and Zammad each contributed two entries to the list. The PHP2Shell vulnerability also earned a place in the catalog, alongside Fortinet, a vendor that has become a recurring name in KEV updates. The volume of additions reflected how quickly attackers moved from disclosure to active abuse, leaving organizations with shrinking windows to patch.

Beyond the KEV additions, active exploitation surfaced across a broad mix of perimeter, application, and endpoint technologies. Network and security appliances from Palo Alto Networks, Cisco, Fortinet, and SonicWall remained prime targets, reinforcing the attacker focus on edge devices that offered direct paths into corporate networks. Exploitation also extended to Redis, MediaWiki, and WordPress Core, exposing databases and widely deployed web platforms to compromise. AMD Radeon Graphics rounded out the list, a reminder that driver and hardware-level components also drew adversary attention during the month.

The ransomware landscape in October was defined by a two-horse race at the top. The Gentlemen claimed the lead with 138 affected organizations, edging out Qilin, which listed 132 victims and maintained the relentless pace seen in previous months. A steep drop followed, with Akira reporting 32 victims, Silent Ransom 30, and Everest 25. Together, the top five groups accounted for 357 affected organizations, with The Gentlemen and Qilin alone responsible for more than 75 percent of that total, signaling a concentration of ransomware activity among a small number of highly active operations.

Vulnerabilities added to the CISA KEV Catalog in October 2026

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
CVE-2026-0322	Palo Alto Networks	PAN-OS	Code Injection vulnerability in Palo Alto Networks that could allow an authenticated attacker with network access to execute arbitrary code with root privileges on the firewall.	Yes	No	False

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
CVE-2026-21589	Atlassian	Multiple Products	Files or Directories Accessible to External Parties vulnerability in Atlassian Multiple Products which could allow an unauthenticated attacker to access specific files within the web application root directory in affected versions.	No	No	False
CVE-2026-41709	Broadcom	VMware ESX	Insufficient Logging vulnerability in Broadcom VMWare ESX that could allow a malicious actor with admin access to perform certain operations without being logged.	Yes	Yes	False
CVE-2026-46300	Linux	Kernel	Initialization of a Variable vulnerability in Linux Kernel that could allow for unintended modification of page-cache-backed data via failure to preserve the shared-fragment marker during socket buffer coalescing, causing ESP input processing to decrypt shared fragments in place. This vulnerability can be chained with CVE-2026-109618 and CVE-2026-109619 to implant PHP webshells and run commands as root.	No	No	True
CVE-2026-48356	Adobe	Commerce and Magento	Unrestricted Upload of File with Dangerous Type vulnerability in Adobe Commerce and Magento that could result in arbitrary code execution in the context of the current user, potentially gaining elevated access or control over the victim's account or session.	No	No	False
CVE-2026-76418	Cisco	Secure Firewall ASA Software and Cisco Secure FTD Software	Unchecked Return Value to NULL Pointer Dereference vulnerability in Cisco Secure Firewall ASA Software and Cisco Secure FTD Software 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-2026-76519	Cisco	Secure Email Gateway	Relative Path Traversal vulnerability in Cisco Secure Email Gateway that could allow an unauthenticated, remote attacker to write arbitrary files on the underlying operating system.	Yes	No	False

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
CVE-2026-88779	Citrix	NetScaler	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in Citrix NetScaler ADC (formerly Citrix ADC) and Citrix NetScaler Gateway (formerly Citrix Gateway) contain an improper restriction of operations within the bounds of a memory buffer vulnerability that could allow for a denial of service.	Yes	No	False
CVE-2026-96652	Plex	Media Server	Server-Side Request Forgery (SSRF) vulnerability in Plex Media Server that could allow an attacker using any X-Plex-Token value to include a full URL in the 'protocol' parameter and force the Plex server to POST to the attacker's chosen destination. This vulnerability can be chained with CVE-2026-96654, CVE-2026-96655, and CVE-2026-96656.	No	No	False
CVE-2026-96654	Plex	Media Server	Improper Neutralization of Encoded URI Schemes in a Web Page vulnerability in Plex Media Server that could allow an attacker to call other plugins' functions and supply their own parameters. This vulnerability can be chained with CVE-2026-96652, CVE-2026-96655, and CVE-2026-96656.	No	No	False
CVE-2026-96655	Plex	Media Server	Server-Side Request Forgery (SSRF) vulnerability in Plex Media Server that could allow an authenticated user to request arbitrary internal or external addresses via the '/video/:/transcode/universal' path parameter. This vulnerability can be chained with CVE-2026-96652, CVE-2026-96654, and CVE-2026-96656.	No	No	False
CVE-2026-96656	Plex	Media Server	External Control of File Name or Path vulnerability in Plex Media Server which can allow an admin user to write arbitrary files that may be executed on load. This vulnerability can be chained with CVE-2026-96652, CVE-2026-96654, and CVE-2026-96655.	No	No	False

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
CVE-2026-96951	Microsoft	Windows	Command Injection vulnerability in Microsoft Windows that allows an unauthorized attacker to bypass a security feature over a network.	Yes	No	False
CVE-2026-97229	GitLab	Community Edition and Enterprise Edition	Integer Overflow or Wraparound vulnerability in GitLab Community Edition and Enterprise Edition that could allow an unauthenticated user to execute arbitrary code on the GitLab server via a specially crafted regular expression in a CI/CD configuration, due to insufficient regular expression validation.	No	No	True
CVE-2026-102489	Zammad GmbH	Zammad	Session Fixation vulnerability in Zammad GmbH Zammad that can lead to remote code execution as the zammad user. This vulnerability can be chained with CVE-2026-102490.	Yes	No	False
CVE-2026-102490	Zammad GmbH	Zammad	Improper Privilege Management vulnerability in Zammad GmbH Zammad that can allow the local zammad user to escalate privileges to root. This vulnerability can be chained with CVE-2026-102489.	Yes	No	False
CVE-2026-102764	BeyondTrust	Remote Support	Authentication Bypass by Spoofing vulnerability in BeyondTrust Remote Support that could allow a remote attacker to perform file operations on the appliance.	Yes	Yes	False
CVE-2026-104286	Fortinet	FortiMail	Path Traversal vulnerability in Fortinet FortiMail that may allow an unauthenticated attacker to write arbitrary files on the underlying system via crafted HTTP or HTTPS requests.	Yes	No	False
CVE-2026-104935	Ivanti	Connect Secure	Authentication Bypass by Spoofing vulnerability in Ivanti Connect Secure that allows a remote unauthenticated attacker to execute arbitrary commands.	Yes	Yes	False
CVE-2026-105133	Ahsay	AhsayCBS	Improper Authentication vulnerability in Ahsay AhsayCBS that could allow a remote attacker to bypass authentication via manipulation of the random parameter in the API component's	No	Yes	False

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
			checkSysPwd function. This vulnerability can be chained with CVE-2026-105134.			
CVE-2026-105134	Ahsay	AhsayCBS	Command Injection vulnerability in Ahsay AhsayCBS that could allow a remote attacker to execute operating system commands via manipulation of the random parameter in the Replication Receiver component's /rps/api/json/UpdateReceivers.do endpoint. This vulnerability can be chained with CVE-2026-105133.	No	Yes	False
CVE-2026-106931	EG Secure Solutions	SiteGuard Server Edition	OS Command Injection vulnerability in EG Secure Solutions SiteGuard Server Edition which may allow an attacker to execute arbitrary OS commands with root or SYSTEM privileges on the system running the affected product.	No	No	False
CVE-2026-109618	PHP Group	PHP	Memory Corruption vulnerability in PHP that allows for unauthenticated remote code execution.	Yes	Yes	True
CVE-2026-109619	PHP Group	PHP	Internal Request-State vulnerability in PHP Stale that allows for unauthenticated remote code execution.	Yes	Yes	True
CVE-2026-110447	Collabora	Collabora Online – Built-in CODE Server	OS Command Injection vulnerability in Collabora Online - Built-in CODE Server that allows for remote code execution when the CODE server isn't running.	No	No	False
CVE-2026-110936	Siemens	Software Center	Uncontrolled Search Path Element vulnerability in Siemens Software Center that could allow an authenticated local attacker to place a specially crafted DLL in a directory that the application searches, leading to arbitrary code execution with the privileges of the affected application.	Yes	No	False

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
CVE-2026-111357	Ivanti	Connect Secure	Missing Authentication for Critical Function vulnerability in Ivanti Connect Secure that could allow a local authenticated attacker to escalate their privileges. This vulnerability can be chained with CVE-2026-104935 and CVE-2026-118527.	Yes	Yes	False
CVE-2026-111497	Google	Brotli	Unchecked Return Value vulnerability in Google Brotli that allows a remote unauthenticated attacker to corrupt adjacent decoder state memory, disclose sensitive memory contents, cause a denial of service, or potentially execute arbitrary code using a crafted Brotli-compressed stream.	No	No	True
CVE-2026-114625	Arista	VeloCloud Orchestrator	SQL Injection vulnerability in Arista VeloCloud Orchestrator 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-2026-118527	Ivanti	Connect Secure	Generation of Predictable Numbers or Identifiers vulnerability in Ivanti Connect Secure that allows a remote authenticated attacker to upload files with attacker-controlled content to a known location on disk. This vulnerability can be chained with CVE-2026-104935 and CVE-2026-111357.	Yes	No	False
CVE-2025-61624	Fortinet	Multiple Products	Path Traversal vulnerability in Fortinet Multiple Products that may allow an authenticated attacker with admin profile and at least read-write permissions to write or delete arbitrary files via specific CLI commands.	No	Yes	True
CVE-2023-22894	Strapi	Strapi	Storage of Sensitive Information vulnerability in Strapi Cleartext that could allow attackers with access to the admin panel to discover sensitive user details via the query filter. The impacted product(s) could be end-of-life (EoL) and/or end-of-service (EoS). Users are	No	No	True

CVE ID	Vendor	Product	Description	Exploited as Zero-day	Malware Abused	OSS
			advised to discontinue use and/or transition to a supported version. This vulnerability can be chained with CVE-2023-22621 to achieve remote code execution.			
CVE-2021-3199	ONLYOFFICE	Docs	Path Traversal vulnerability in ONLYOFFICE Docs Server that can occur when JWT is used, via a /.. sequence in an image upload parameter and could allow for remote code execution.	No	No	False
CVE-2016-3081	Apache	Struts	Command Injection vulnerability in Apache Struts that could allow remote attackers to execute arbitrary code via method:prefix when Dynamic Method Invocation is enabled.	No	No	True
CVE-2015-3306	ProFTPD	ProFTPD	Improper Access Control vulnerability in ProFTPD that could allow remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.	No	No	True
CVE-2015-5477	ISC	BIND	Data Processing Errors vulnerability in ISC BIND that could allow remote attackers to cause a denial of service via TKEY queries.	No	No	True

Actively Exploited Vulnerabilities in October 2026

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-0257	Palo Alto Networks	PAN-OS	Authentication Bypass vulnerability in Palo Alto Networks PAN-OS that allows attackers to bypass security restrictions and establish an unauthorized VPN connection.	No	Yes	False
CVE-2026-20127	Cisco	Catalyst SD-WAN Controller and Manager	Authentication Bypass vulnerability in Cisco Catalyst SD-WAN Controller and Manager	No	Yes	False
CVE-2026-25243	Redis	Redis RESTORE command	Invalid Memory Access vulnerability in Redis RESTORE that allows an authenticated attacker with permission to run RESTORE to achieve remote code execution in the context of the Redis server	No	No	True
CVE-2026-35616	Fortinet	FortiClient EMS	Improper Access Control vulnerability in Fortinet	No	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			FortiClient EMS that may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests.			
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	Yes	False
CVE-2026-85097	Bricksforge	The Bricksforge plugin for WordPress	Unauthenticated Arbitrary File Upload vulnerability in the Bricksforge plugin for WordPress resulting in remotecode execution.	No	No	False
CVE-2026-93836	WPC Product	Bundles for WooCommerce plugin for WordPress	Stored Cross-Site Scripting vulnerability in WPC Product Bundles for WooCommerce plugin for WordPress due to insufficient input sanitization and output escaping.	No	No	False
CVE-2026-94504	Kstover	Ninja Forms - Contact Form Builder with Calculators, Quizzes, Signatures & AI Form Builder WordPress plugin	Stored Cross-Site Scripting vulnerability in Ninja Forms - Contact Form Builder with Calculators, Quizzes, Signatures & AI Form Builder WordPress plugin	No	No	False
CVE-2026-100382	MediaWiki	External Data extension	Unauthenticated Remote Code Execution in MediaWiki External Data extension.	No	No	False
CVE-2026-102255	SonicWall	SMA1000 Series Appliances	Server-Side Request Forgery vulnerability in SonicWall SMA1000 that could allow a remote attacker "to direct the appliance to issue requests on their behalf and reach internal functionality and perform unauthorized operations".	No	No	False
CVE-2026-102785	YOOtheme	YOOtheme Pro framework	Unauthenticated Remote Code Execution vulnerability in YOOtheme Pro framework	No	No	False
CVE-2026-106173	Fortinet	FortiSIEM	Path Traversal vulnerability in Fortinet FortiSIEM that could allow an unauthenticated attacker to execute unauthorized code or commands via specially crafted packets.	No	No	False
CVE-2026-106931	EG Secure Solutions	SiteGuard Server	OS Command Injection Vulnerability in EG Secure Solutions SiteGuard Server that may allow an attacker to execute arbitrary OS commands with root or SYSTEM privileges	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			on the system running the affected product.			
CVE-2026-110447	Nextcloud	Collabora Online Built-in CODE Server app	OS Command Injection vulnerability in Nextcloud Collabora Online Built-in CODE Server app that lets unauthenticated attackers plant PHP webshells on exposed servers.	No	No	False
CVE-2026-116779	WordPress	Core	Remote Code Execution vulnerability in WordPress Core that allows unauthenticated attackers to execute arbitrary code during core upgrades.	No	No	False
CVE-2026-116690	MLflow	MLflow	Path Traversal vulnerability in MLflow that lets unauthenticated users read files from the server.	No	Yes	False
CVE-2026-118539	Drupal	Commerce Core	Missing Authorization vulnerability in Drupal Commerce Core leading to access bypass.	No	No	False
CVE-2024-57727	SimpleHelp	SimpleHelp	Path Traversal Vulnerability in SimpleHelp that allow unauthenticated remote attackers to download arbitrary files from the SimpleHelp host via crafted HTTP requests. These files may include server configuration files and hashed user passwords.	No	Yes	False
CVE-2024-58388	Sharp and Toshiba	Multiple Multifunction Printers	Local File Inclusion vulnerability in Sharp and Toshiba Tec Multiple Multifunction Printers	No	No	False
CVE-2023-20598	AMD	AMD Radeon Graphics kernel driver	Improper Privilege Management in AMD Radeon Graphics driver that can result in arbitrary code execution.	No	Yes	False

Ransomware Insights for October 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 October 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	138	• Manufacturing • Construction • Healthcare • Insurance	• CVE-2025-7771 • CVE-2025-32433 • CVE-2025-33073 • CVE-2025-55182 • CVE-2024-55591

Ransomware	Description	No of affected organizations in October 2026	Targeted Industries	Vulnerabilities abused most
	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.		• Consumer Services	
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.	132	• 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
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.	32	• 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 October 2026	Targeted Industries	Vulnerabilities abused most
Silent Ransom Group	Silent Ransom Group (SRG; aka Luna Moth, Chatty Spider, UNC3753, Storm-0252, leak-site brand LeakedData) first surfaced in March 2022 as a financially-motivated splinter of the dismantled Conti syndicate. Its targets are overwhelmingly US-based professional-services organizations - law firms above all, plus insurance, accounting/CPA, finance, and (per FBI) healthcare, with a handful of posted victims in Canada, Germany, the UK and Russia, and named hits including Marriott-linked data, and law firms such as Jones Day, Orrick, and Fenwick appearing on its leak site. Delivery is human-driven rather than technical: benign invoice/subscription email lures and direct vishing calls in which operators impersonate internal IT helpdesk staff, steer victims to install legitimate RMM tools and when remote attempts fail, send a person on-site to copy data to a USB/external drive. Critically, SRG performs no encryption, so there is no cipher, no appended file extension, and no dropped ransom-note filename the note is an unbranded extortion email demanding payment within three days under threat of publication.	30	• Insurance • Healthcare • Retail • Energy • Consulting	Unknown
Everest	Everest is a Russian-speaking closed-group ransomware operation that emerged in December 2020 as a data exfiltration group and evolved into full ransomware by early 2021, encrypting Windows hosts with a combination of AES and DES encryption and appending the .everest extension to affected files. The group ran three parallel revenue streams: double extortion attacks backed by a Tor leak site with countdown timers and staged data releases, an initial access brokerage service selling compromised network access and	25	• Non-profit organization • Finance • Food & Beverage • Information Technology • Legal • Manufacturing	• CVE-2026-49994 • CVE-2024-4947 • CVE-2024-21762 • CVE-2024-55591 • CVE-2023-36884

Ransomware	Description	No of affected organizations in October 2026	Targeted Industries	Vulnerabilities abused most
	harvested credentials to other threat actors since November 2021, and a corporate insider recruitment program launched in October 2023 that offered cash payments and profit-sharing to employees willing to provide remote access to organizations in the United States, Canada and Europe.			
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.	23	• Education • Healthcare • Government • Manufacturing • Information	• CVE-2025-4427 • CVE-2025-4428 • CVE-2025-5777 • CVE-2025-8088 • CVE-2025-10585
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.	22	• Business Services • Manufacturing • Technology • Healthcare • Construction	Unknown
Play	Play ransomware was first seen in June 2022, targeting organizations through various initial access	18	• Government • Education • Healthcare	• CVE-2025-8088 • CVE-2025-29824 • CVE-2025-31161

Ransomware	Description	No of affected organizations in October 2026	Targeted Industries	Vulnerabilities abused most
	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.		• Media • Information Technology	• CVE-2025-31324 • CVE-2025-53770
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 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.	15	• Business Services • Consumer Servies • Manufacturing • Technology • Public Sector	Unknown
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	12	• 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 October 2026	Targeted Industries	Vulnerabilities abused most
	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.			

Conclusion

October proved that awareness campaigns alone could not outpace adversaries who weaponized flaws within days of disclosure and drove ransomware victim counts into the hundreds. The month showed that organizations needed to prioritize KEV-listed vulnerabilities, harden internet-facing edge devices, and pair rapid patching with continuous exposure monitoring to stay ahead of exploitation. Defenders who moved from reactive patch cycles to intelligence-driven prioritization stood the best chance of shrinking the attack window. LOVI supported that shift by delivering timely, actionable vulnerability and threat intelligence that helped security teams focus on the risks that mattered most.

loginsoft

Connect with us

linkedin.com/loginsoft

x.com/loginsoft_inc

www.loginsoft.com