loginsoft

Monthly Report

Threat & Vulnerabilities Report – October 2025

Summary

October, recognized as Cybersecurity Awareness Month, underscored the critical importance of vigilance and patch discipline across industries. Throughout the month, 32 vulnerabilities were added to the CISA Known Exploited Vulnerabilities (KEV) catalog, a clear indication of rising real-world exploitation.

Microsoft topped the list with 8 confirmed exploited CVEs, while Apple, Kentico, Adobe, and Dassault Systèmes each accounted for 2 vulnerabilities, underscoring adversaries continued focus on core operating environments, enterprise applications, and e-commerce platforms. Beyond major vendors, the KEV additions spanned a diverse range of technologies from SmartBedded Metrobridge, Samsung, Jenkins, Juniper, Oracle, Mozilla, Linux, Synacor, SKYSEA, Grafana Labs, Rapid7, IGEL, Motex, and others reinforcing that no segment of the technology supply chain is immune.

Ransomware operations continued to intensify, with Qilin, Akira, and Sinobi driving major incidents across the threat landscape. Key sectors including education, healthcare, and finance remained prime targets, as adversaries weaponized both known and newly surfaced vulnerabilities to infiltrate networks, encrypt systems, exfiltrate data, and disrupt critical services.

Actively Exploited Vulnerabilities

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	CISA KEV	OSS
CVE-2025-2746	Kentico	Xperience CMS	An Authentication Bypass Using an Alternate Path or Channel Vulnerability in the Kentico Xperience CMS that could allow an attacker to control administrative objects.	No	No	Yes	False
CVE-2025-2747	Kentico	Xperience CMS	An Authentication Bypass Using an Alternate Path or Channel Vulnerability in the Kentico Xperience CMS that could allow an attacker to control administrative objects.	No	No	Yes	False
CVE-2025-4008	Smartbedded	Meteobridge	A Command Injection Vulnerability in the Smartbedded Meteobridge that enables remote unauthenticated attackers to gain arbitrary command execution with elevated privileges on affected devices.	No	No	Yes	False
CVE-2025-5947	Themeforest	Service Finder Bookings	An Authentication Bypass Vulnerability in the Service Finder Bookings plugin for	No	No	No	False

		(WordPress plugin)	WordPress that enables unauthenticated attackers to login as any user including admins.				
CVE-2025-6204	Dassault Systemes	DELMIA Apriso	A Code Injection Vulnerability in the Dassault Systemes DELMIA Apriso that could allow an attacker to execute arbitrary code	No	No	Yes	False
CVE-2025-6205	Dassault Systemes	DELMIA Apriso	A Missing Authorization Vulnerability in the Dassault Systemes DELMIA Apriso that could allow an attacker to gain privileged access to the application.	No	No	Yes	False
CVE-2025-6264	Rapid7	Velociraptor	An Incorrect Default Permissions Vulnerability in the Rapid7 Velociraptor that can lead tno arbitrary command execution and endpoint takeover.	No	No	Yes	True
CVE-2025-6388	Theme Spirit	Spirit Framework (WordPress plugin)	An Authentication Bypass Vulnerability in the Spirit Framework plugin for WordPress that allows attackers to bypass authentication, seize control of accounts and escalate privileges.	No	No	No	False
CVE-2025-11533	Apsus	WP Freeio plugin	A Privilege Escalation Vulnerability in the WP Freeio plugin for WordPress that allows unauthenticated attackers to create administrator accounts simply by manipulating the user-role field during registration.	No	No	No	False
CVE-2025-21043	Samsung	Mobile Devices	An Out-of-Bounds Write Vulnerability in the Samsung libimagecodec.quram.so component that could lead to arbitrary code execution	Yes	No	Yes	False
CVE-2025-41244	Broadcom	VMware Aria Operations and VMware Tools	A Privilege Defined with Unsafe Actions Vulnerability in Broadcom VMware Aria Operations and VMware Tools allows a low-privilege user on a VM to escalate privileges to root by exploiting an	No	No	Yes	False

			untrusted search path in the get-versions.sh script used for service discovery.				
CVE-2024-24893	XWiki	XWiki	A Remote Code Execution Vulnerability in the XWiki, that allows unauthenticated attackers to inject malicious templates and execute arbitrary code.	No	No	Yes	False
CVE-2025-24990	Microsoft	Windows	An Untrusted Pointer Dereference Vulnerability in Microsoft Windows that allows for privilege escalation.	Yes	No	Yes	False
CVE-2025-27915	Synacor	Zimbra Collaboratio n Suite	A Cross-Site Scripting (XSS) Vulnerability in the Zimbra Collaboration that can result in arbitrary code execution.	No	No	Yes	False
CVE-2025-33073	Microsoft	Windows	An Improper Access Control Vulnerability in the Microsoft Windows SMB Client that could allow for privilege escalation.	No	No	Yes	False
CVE-2025-47827	IGEL	IGEL OS	A Use of a Key Past its Expiration Date Vulnerability in the IGEL OS allows for a secure boot bypass.	No	No	Yes	False
CVE-2025-54236	Adobe	Commerce and Magento	An Improper Input Validation in the Adobe Commerce and Magento allows an attacker to take over customer accounts through the Commerce REST API.	No	No	Yes	True
CVE-2025-54253	Adobe	Experience Manager	A Code Execution Vulnerability in the Adobe Experience Manager Forms enables for arbitrary code execution.	No	No	Yes	False
CVE-2025-59230	Microsoft	Windows	An Improper Access Control Vulnerability in the Microsoft Windows Remote Access Connection Manager that allows an authorized attacker to elevate privileges locally.	Yes	No	Yes	False
CVE-2025-59287	Microsoft	Windows	A Deserialization of Untrusted Data Vulnerability in the	No	No	Yes	False

			Microsoft Windows Server Update Service (WSUS).				
CVE-2025-61882	Oracle	E-Business Suite	An Unspecified Vulnerability in Oracle E-Business Suite that could enable an unauthenticated attacker with network access via HTTP to compromise and take control of the Oracle Concurrent Processing component.	Yes	Yes	Yes	False
CVE-2025-61884	Oracle	E-Business Suite	A Server-Side Request Side Forgery vulnerability in the Oracle E-Business Suite that is remotely exploitable without authentication i.e., it may be exploited over a network without the need for a username and password.	No	Yes	Yes	False
CVE-2024-9234	Wpmet	GutenKit WordPress plugin	An Unauthenticated Arbitrary File Upload Vulnerability in the GutenKit plugin for WordPress that enables unauthenicated attackers to install and activate arbitrary plugins.	No	No	No	False
CVE-2024-9707	ThemeHunk	Hunk Companion	A Missing Authorization to Unauthenticated Arbitrary Plugin installation/activation vulnerability in the Hunk Companion that allows unauthenticated attackers to install and activate arbitrary plugins.	No	No	No	False
CVE-2024-11972	ThemeHunk	Hunk Companion plugin	A Remote Code Execution Vulnerability in the Hunk Companion WordPress plugin that allows unauthenticated attackers to install plugins without authorization.	No	No	No	False
CVE-2023-43261	Milesight	Industrial Cellular Routers	An Information Disclosure Vulnerability in the Milesight industrial cellular routers that enables attackers to access sensitive router components.	No	No	No	False
CVE-2022-48503	Apple	Multiple Products	An Unspecified Vulnerability in Apple	No	No	Yes	True

			multiple products that may lead to arbitrary code execution.				
CVE-2021-22555	Linux	Kernel	An Out-of-Bounds Write Vulnerability in the Linux Kernel that allows an attacker to gain privileges or cause a DoS through user name space.	No	No	Yes	True
CVE-2021-43226	Microsoft	Windows	A Privilege Escalation Vulnerability in Microsoft Windows that enables a local, privileged attacker to bypass certain security mechanisms.	No	No	Yes	False
CVE-2021-43798	Grafana Labs	Grafana	A Path Traversal Vulnerability in Grafana that enables an attacker to access local files.	No	No	Yes	True
CVE-2017-1000353	Jenkins	Jenkins	A Remote Code Execution Vulnerability in the Jenkins allows attackers to transfer a serialized Java SignedObject object to the remoting-based Jenkins CLI, that would be deserialized using a new ObjectInputStream, bypassing the existing blacklist-based protection mechanism.	No	Yes	Yes	True
CVE-2016-7836	SKYSEA	Client View	An Improper Authentication Vulnerability in the SKYSEA Client View enables remote code execution via a flaw in processing authentication on the TCP connection with the management console program.	No	Yes	Yes	False
CVE-2015-7755	Juniper	ScreenOS	An Improper Authentication Vulnerability in the Juniper ScreenOS that enables an unauthorized remote administrative access to the device	No	No	Yes	False
CVE-2014-6278	GNU	GNU Bash	An OS Command Injection Vulnerability in the GNU Bash enables remote attackers to execute arbitrary commands via a crafted environment.	No	No	Yes	False

CVE-2013-3918	Microsoft	Windows	An Out-of-Bounds Write Vulnerability in Microsoft Windows enables an attacker to exploit the vulnerability by constructing a specially crafted webshell.	Yes	Yes	Yes	False
CVE-2011-3402	Microsoft	Windows	A Remote Code Execution Vulnerability in Microsoft Windows that enables remote attackers to execute arbitrary code via crafted font data in a Word document or web page.	No	Yes	Yes	False
CVE-2010-3765	Mozilla	Multiple Products	A Remote Code Execution Vulnerability in Mozilla multiple products that can trigger memory corruption.	No	Yes	Yes	True
CVE-2010-3962	Microsoft	Internet Explorer	An Uninitialized Memory Corruption Vulnerability in the Microsoft Internet Explorer that can lead to remote code execution	No	Yes	Yes	False

Ransomware Insights for October 2025

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 for October	Targeted Industries	Vulnerabilities Abused Most
Qilin	The Qilin ransomware has been in existence since August 2022, also recognized as Agenda, and 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.	190	• Education • Healthcare	• CVE-2025-31324 • CVE-2024-21762 • CVE-2024-55591 • CVE-2023-27532
Akira	Akira ransomware underscored a critical security vulnerability linked to the lack of Multi-Factor Authentication	70	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259

	(MFA). The nations experiencing the fallout encompass the United States, the United Kingdom, Canada, Australia, and South Korea. The repercussions are noteworthy, especially within pivotal domains like Services and Goods, Manufacturing, Education, and Finance.			
Sinobi	Sinobi ransomware is a sophisticated threat, suspected to be a rebrand of the Lynx ransomware group, employing double-extortion tactics that exfiltrate sensitive data before encrypting systems using Curve-25519 and AES-128-CTR algorithms. It has targeted a wide range of industries, including healthcare, manufacturing, legal services, education, and construction/engineering, highlighting its broad attack strategy. To mitigate risk, organizations are advised to implement multi-factor authentication, secure VPN access, keep systems updated with patches, train employees on phishing and safe practices, maintain offline backups, and monitor network activity for unusual behavior.	62	• Healthcare • Manufacturing • Legal Services • Education • Construction	Unknown
Inc Ransom	Inc. ransomware, which emerged in June 2023, spread through spear-phishing emails and targeted vulnerable services, such as the exploitation of **CVE-2023-3519** in Citrix NetScaler. Our observations indicate that Inc. ransomware has deliberately targeted a range of sectors, including healthcare, education, and government entities. This ransomware operates as a multi-extortion scheme, involving the theft of victim data and threats to release the data online unless the victim complies with their demands.	28	• Education • Healthcare • Government sectors	• CVE-2023-3519
Play	The Play ransomware group, also identified as Balloonfly and PlayCrypt, has significantly impacted businesses and critical infrastructure across North America, South America and Europe regions. With a primary focus on telecommunications, the group has extended its reach to healthcare,	22	• Healthcare • Media • Technology • Telecommunication	• CVE-2022-41040 • CVE-2022-41080 • CVE-2022-41082 • CVE-2021-34523 • CVE-2020-12812 • CVE-2018-13379

	technology and media industries. It was observed that the group focused on managed service providers (MSPs) globally, using remote monitoring and management (RMM) tools to infiltrate customer systems. Their campaigns involve custom tools like "Grixba" and "VSS Copying Tool" written in .NET. Interestingly, Play ransomware affiliates prefer email communication for negotiations and do not provide Tor negotiation page links in ransom notes on compromised systems.			
Medusa	Emerging in 2019, the Medusa ransomware operates on a ransomware-as-a-service (RaaS) model and has been observed infecting and encrypting systems in various sectors, notably focusing on the healthcare sector. Attackers typically gain initial access through brute-force assaults on Remote Desktop Protocol (RDP), exploiting leaked RDP credentials, or employing spear-phishing tactics to acquire user credentials. Notably, ransomware affiliates have been leveraging the infrastructure of the United States, potentially indicating preparations for future attacks.	15	• Healthcare • Finance • Technology • Manufacturing	• CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-34362 • CVE-2023-47246 • CVE-2022-2295
Lynx	Lynx ransomware, active since mid-2024, is a sophisticated malware operating under a ransomware-as-a-service (RaaS) model, claiming over 20 victims across various industries. It employs single and double extortion tactics, encrypting critical files with a ".lynx" extension and threatening to leak data if ransoms are unpaid, while also deleting backups like shadow copies to hinder recovery. Notably, Lynx has targeted organizations in the United States, United Kingdom, Canada, Guatemala, and Australia, with a significant attack on Romania's Electrica Group, demonstrating its capacity to disrupt critical infrastructure. The ransomware employs a hybrid encryption method, using AES for file encryption and RSA for key protection, and directs victims	14	• Finance • Retail • Real Estate • Manufacture • Construction • Logistic	Unknown

	to Tor communication channels for ransom negotiations. Key features include targeting specific directories for encryption, terminating processes, encrypting network drives, escalating privileges, and altering system settings, such as background images. By employing these sophisticated techniques, Lynx continues to pose a serious threat to industries worldwide.			
Safepay	SafePay is a newly emerging ransomware strain believed to be derived from leaked LockBit source code, distinguished by its ransom note titled "readme_safepay.txt" and encrypted file extensions labeled ".safepay." While bearing similarities to LockBit, SafePay's refined approach establishes it as a formidable new player in the ransomware landscape. It employs a two-phase attack strategy involving initial system infiltration followed by data encryption, often using anti-detection mechanisms to evade security measures. Linked to the LockBit ransomware builder, SafePay is suspected to involve experienced cybercriminals in its creation and deployment. The ransomware primarily targets payment processors and banks, posing a significant threat to financial institutions. With at least 22 victims reported so far, SafePay's sophisticated techniques for spreading and exfiltrating data underscore its potency and highlight the challenges of mitigating its impact.	14	• Education • Finance • Agriculture • Manufacturing • Healthcare • Logistic	Unknown
Rhysida	Rhysida ransomware has a new variant that provides Ransomware-as-a-service (RaaS). As of 2023, approximately 50 victims have been identified, targeting the Education, Healthcare, Manufacturing, Information Technology and Government sectors. The deployment of Rhysida involves various methods, including the use of Cobalt Strike or a similar framework, as well as phishing campaigns. Notably, we have observed the threat actor exploiting	13	• Education • Healthcare • Manufacturing • Information Technology • Government sectors	• CVE-2020-1472

	Zerologon's (CVE-2020-1472) vulnerability, a critical elevation of privileges flaw in Microsoft's Netlogon Remote Protocol. Upon gaining network access, the Rhysida gang employs Living off the Land Binaries (LoLBins) techniques to execute malicious activities discreetly and avoid detection.			
Clop	Clop ransomware is a sophisticated cyber threat first identified in 2019, known for its double-extortion tactics and targeted attacks on large organizations. Operated by the financially motivated cybercrime group TA505, Clop not only encrypts victim data but also exfiltrates sensitive information, threatening public disclosure unless a ransom is paid. The ransomware has been linked to high-profile attacks exploiting vulnerabilities in widely used software, including the MOVEit Transfer and Accellion File Transfer Appliance (FTA). Clop operators gain initial access through phishing campaigns, exploiting zero-day vulnerabilities, or leveraging compromised credentials.	11	• Healthcare • Bank • Education • Gaming • Transportation	• CVE-2024-55956 • CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-34362 • CVE-2023-47246
Handala	Handala is a politically motivated ransomware group active since late 2023, primarily targeting Israeli organizations across critical sectors such as energy, healthcare, government, education, and defense, with spillover attacks affecting U.S. infrastructure and other countries including Canada, Germany, and Australia. Known for blending ransomware with wiper tactics and data leaks, the group uses politically charged messaging to justify its campaigns, often tied to the Israel-Palestine conflict. High-profile incidents include breaches of Israeli energy firms, hospitals, academic institutions, and defense-linked companies, with stolen data volumes reaching terabytes and ransom demands up to 8 BTC. Handala's operations reflect a mix of ideological hacktivism and disruptive intent,	7	• Healthcare • Energy • Manufacturing • Government sector • Education • Defense	Unknown

	positioning it as a serious threat to critical infrastructure globally.			

Conclusion

As Cybersecurity Awareness Month comes to an end, one message stands clear: real-world exploitation is accelerating, and reactive security is no longer enough. Staying ahead now demands rapid patching, intelligence-led defense, and proactive exposure management to counter increasingly agile threat actors. Platforms like Loginsoft Vulnerability Intelligence (LOVI) empower security teams with real-time exploit insights, threat actor tracking, and actionable intelligence, enabling faster detection and response in an ever-evolving threat landscape.