loginsoft

Monthly Report

Threat & Vulnerabilities Report – September 2025

Executive Summary

September marked a turbulent month in the cybersecurity landscape, with a sharp rise in zero-day activity and renewed focus on high-impact vulnerabilities across major vendors. A total of 16 vulnerabilities were added to the CISA Known Exploited Vulnerabilities (KEV) catalog, reflecting the continued trend of adversaries rapidly exploiting both newly disclosed and long-standing flaws.

The month's additions included three vulnerabilities each from Cisco and TP-Link, underscoring the ongoing targeting of networking and infrastructure devices that form the backbone of enterprise and home environments. Other affected vendors included Sudo, Fortra, Libraesva, Google, Adminer, Linux, Android, Sitecore, and Meta Platforms, representing a wide cross-section of technologies spanning software, cloud, and IoT ecosystems.

Notably, 12 of these vulnerabilities were actively exploited as zero-days, emphasizing the accelerating speed at which threat actors weaponize unpatched flaws.

Meanwhile, ransomware activity continued its aggressive momentum, with Qilin, Akira, and IncRansom leading the charge. The education, healthcare, and finance sectors were among the most heavily affected, as adversaries leveraged both known and emerging vulnerabilities to deploy ransomware payloads, exfiltrate data, and disrupt operations.

Actively Exploited Vulnerabilities

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	CISA KEV	OSS
CVE-2025-5086	Dassault Systèmes	DELMIA Apriso	Deserialization of Untrusted Data Vulnerability in DELMIA Apriso that can lead to remote code execution.	No	No	Yes	False
CVE-2025-5821	WordPress	Case Theme User plugin	An Authentication Bypass Vulnerability in the Case Theme User WordPress plugin that enables unauthenticated attackers to log in as administrative users, and access admin user emails.	No	No	No	False
CVE-2025-9377	TP-Link	Multiple Routers	An OS Command Injection Vulnerability in TP-Link Archer C7(EU) and TL-WR841N/ND(MS) that exists in the Parental Control page.	Yes	Yes	Yes	False
CVE-2025-10035	Fortra	GoAnywhere MFT	A Deserialization Vulnerability in the License servlet of Fortra's GoAnywhere MFT	Yes	No	Yes	False

			solution and allows an attacker to achieve unauthenticated remote code execution.				
CVE-2025-10585	Google	V8 JavaScript engine	A Type Confusion Vulnerability in the Google Chrome V8 JavaScript Engine and WebAssembly engine.	Yes	No	Yes	False
CVE-2025-20333	Cisco	Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense	A Buffer Overflow Vulnerability in the Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) that allows for remote code execution.	Yes	Yes	Yes	False
CVE-2025-20352	Cisco	• IOS • IOS XE Software	A Denial of Service and Remote Code Execution Vulnerability in the Cisco IOS and IOS XE software that enables an attacker to execute arbitrary code as the root user and take full control of the affected device.	Yes	No	Yes	False
CVE-2025-20362	Cisco	Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense	A Missing Authorization Vulnerability in the Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense that can allow an attacker to access a restricted URL without any authentication.	Yes	Yes	Yes	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	No	False
CVE-2025-32463	Sudo	Sudo	An Inclusion of Functionality from Untrusted Control Sphere Vulnerability in the Sudo that could allow an attacker to run arbitrary commands as root on systems that support ***/etc/nsswitch.conf***.	No	No	Yes	False
CVE-2025-38352	Linux	Kernel	A Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability in	Yes	No	Yes	True

			the Linux Kernel that impacts confidentiality, integrity and availability.				
CVE-2025-41244	Broadcom	• VMware Tools • VMware Aria Operations	A Local Privilege Escalation Vulnerability in the VMware Aria Operations and VMware Tools.	Yes	Yes	No	False
CVE-2025-42957	SAP SE	SAP S/4HANA (private cloud and on-premise editions)	A Command Injection Vulnerability in the SAP S/4HANA enables an attacker with user privileges to exploit a vulnerability function module exposed via RFC.	No	No	No	False
CVE-2025-48543	Android	Runtime	A Use-After-Free Vulnerability in the Android Runtime that could lead to privilege escalation.	Yes	No	Yes	False
CVE-2025-51591	JGM	Pandoc	A Server-Side Request Forgery in the JGM Pandoc that allows attacker to gain access and compromise the whole infrastructure via injecting a crafted iframe.	No	No	No	False
CVE-2025-53690	Sitecore	Multiple Products	Deserialization of Untrusted Data Vulnerability in Sitecore Multiple Products that could result in remote code execution.	Yes	Yes	Yes	False
CVE-2025-55177	Meta Platforms	WhatsApp	An Incorrect Authorization Vulnerability in WhatsApp due to an incomplete authorization of linked device synchronization messages.	Yes	No	Yes	False
CVE-2025-59689	Libraesva	Email Security Gateway	A Command Injection Vulnerability via a compressed email attachment in the Libraesva Email Security Gateway	No	No	Yes	False
CVE-2024-7344	Howyar	Howyar UEFI Application	A Remote Code Execution Vulnerability in the Howyar Reloader UEFI application that could lead to a secure boot bypass.	No	Yes	No	False

CVE-2024-40766	SonicWall	SonicOS	An Improper Access Control Vulnerability in the SonicWall SonicOS that could lead to unauthorized resource access and under certain conditions can result in firewall crash.	No	Yes	Yes	False
CVE-2023-50224	TP-Link	TL-WR841N	An Authentication Bypass by Spoofing Vulnerability in TP-Link TL-WR841N leading to stored credentials disclosure.	No	Yes	Yes	False
CVE-2021-21311	Adminer	Adminer	A Server-Side Request Forgery Vulnerability in the Adminer, that when exploited, allows a remote attacker to obtain potentially sensitive information.	No	No	Yes	True
CVE-2020-24363	TP-Link	TL-WA855RE	A Missing Authentication for Critical Function Vulnerability in TP-link TL-WA855RE that enables an unauthenticated attacker to submit a TDDP_RESET POST request for a factory reset and reboot.	No	No	Yes	False

Ransomware Insights

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 September	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,	74	• Education • Healthcare	• CVE-2025-31324 • CVE-2024-21762 • CVE-2024-55591 • CVE-2023-27532

	particularly in nations such as Thailand and Indonesia.			
Akira	Akira ransomware underscored a critical security vulnerability linked to the lack of Multi-Factor Authentication (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.	52	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259
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.	38	• 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, 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.	36	• Healthcare • Media • Technology • Telecommunication	• CVE-2022-41040 • CVE-2022-41080 • CVE-2022-41082 • CVE-2021-34523 • CVE-2020-12812 • CVE-2018-13379

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 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.	26	• Finance • Retail • Real Estate • Manufacture • Construction • Logistic	Unknown
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	17	• Education • Finance • Agriculture • Manufacturing • Healthcare • Logistic	Unknown

	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.			
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.	9	• Government entities • Infrastructure sectors	• CVE-2024-57726 • CVE-2024-57727 • CVE-2024-57728 • CVE-2022-26134

Conclusion

In conclusion, September's cybersecurity trends highlight a rapidly evolving threat landscape where speed, precision, and intelligence define both attack and defense. The rise in zero-day exploits and the persistence of ransomware operations show that adversaries are becoming faster and more strategic, often chaining vulnerabilities for maximum impact. To counter this, organizations must move beyond reactive patching toward proactive, intelligence-driven defense. Loginsoft Vulnerability Intelligence (LOVI) meets this need by delivering real-time, actionable insights that help organizations anticipate threats, prioritize vulnerabilities, and strengthen defenses, ensuring resilience and protection in an increasingly complex cyber environment.

External References:

- https://www.cisa.gov/news-events/alerts/2025/09/02/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/09/03/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/09/04/cisa-adds-three-known-exploited-vulnerabilities-catalog

- https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/ongoing-active-exploitation-of-sonicwall-ssl-vpns-in-australia
- https://blog.sekoia.io/solving-the-7777-botnet-enigma-a-cybersecurity-quest/
- https://www.cisa.gov/news-events/alerts/2025/09/25/cisa-directs-federal-agencies-identify-and-mitigate-potential-compromise-cisco-devices
- https://www.cisa.gov/news-events/directives/ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices
- https://security.samsungmobile.com/securityUpdate.smsb
- https://www.cisa.gov/news-events/alerts/2025/09/11/cisa-adds-one-known-exploited-vulnerability-catalog
- https://thehackernews.com/2025/09/fortra-goanywhere-cvss-10-flaw.html
- https://thehackernews.com/2025/09/google-patches-chrome-zero-day-cve-2025.html

loginsoft

Connect with us

linkedin.com/loginsoft

x.com/loginsoft_inc

www.loginsoft.com