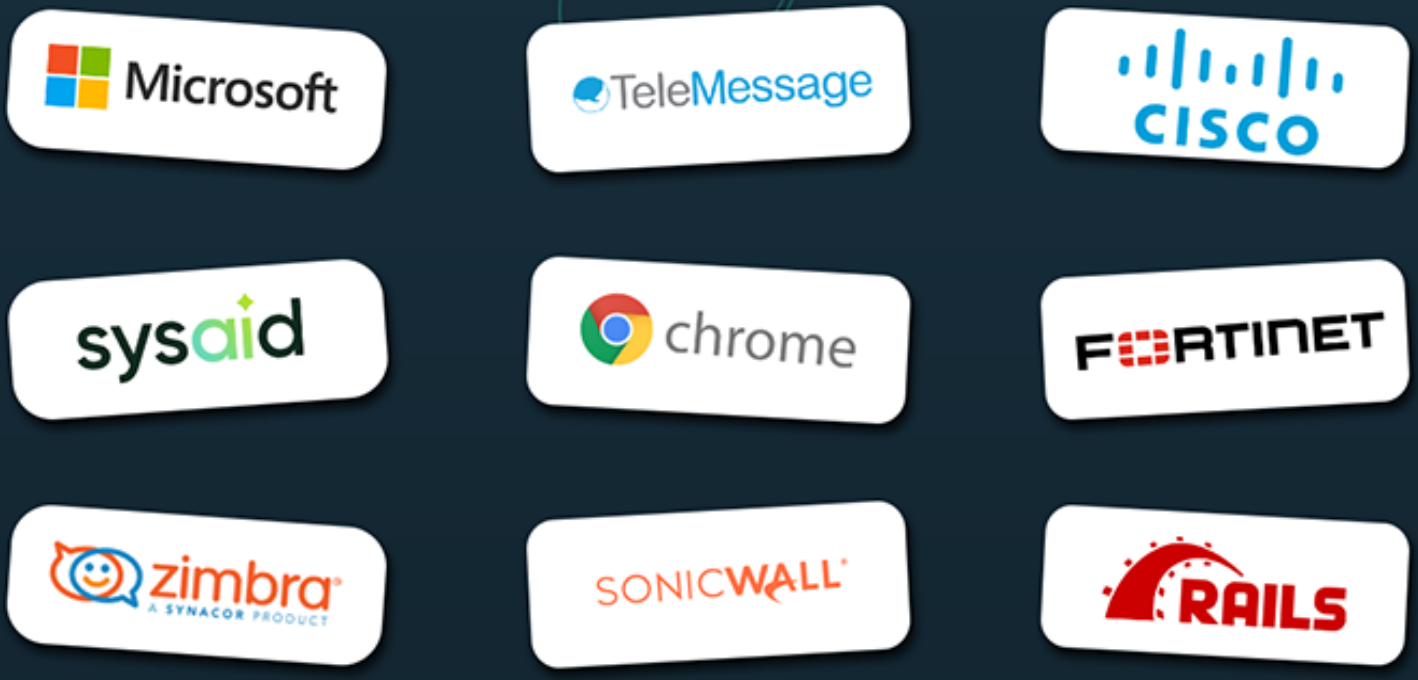
loginsoft

Monthly Report

Threat & Vulnerabilities Report – July 2025



Executive Summary

With threat actors accelerating their focus on widely used enterprise software, the pace of exploitations continues to rise, highlighting the urgency for swift vulnerability management across organizations. In July, a total of 20 vulnerabilities were added to the CISA's Known Exploited Vulnerabilities (KEV) catalog, with five of them actively exploited as zero-days.

Microsoft topped the list with three critical flaws, followed by two vulnerabilities from TeleMessage's TM SGNL platform reportedly used by a former U.S. National Security Advisor. Cisco, SysAid, and Google each accounted for two high-impact entries, emphasizing the increasing threat posed to enterprise ecosystems across communication, infrastructure, and productivity platforms.

Meanwhile, ransomware activity remained persistent. Qilin, IncRansom, and Akira were among the most active groups this month. The most affected sectors included education, healthcare, and manufacturing, with attackers leveraging unpatched systems and VPN access to execute double extortion and data encryption operations.

Actively Exploited Vulnerabilities

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	CISA KEV	OSS
CVE-2025-2775	SysAid	SysAid On-Prem	An Improper Restriction of XML External Entity Reference Vulnerability in the SysAid On-Prem in the **Checkin processing functionality** enables administrator account takeover.	No	No	Yes	False
CVE-2025-2776	SysAid	SysAid On-Prem	An Improper Restriction of XML External Entity Reference Vulnerability in the SysAid On-Prem in the **Server URL processing functionality** enables administrator account takeover.	No	No	Yes	False
CVE-2025-5394	Bearsthemes	Alone - Charity Multipurpose Non-profit	An Arbitrary File Upload Vulnerability in the Alone - Charity Multipurpose Non-	No	No	No	False

		WordPress Theme	profit WordPress Theme for WordPress that enables unauthenticated attackers to upload arbitrary files and achieve remote code execution.				
CVE-2025-5777	Citrix	NetScaler ADC and Gateway	An Out-of-Bounds Read Vulnerability in the Citrix NetScaler ADC and Gateway that arises due to insufficient input validation.	No	No	Yes	False
CVE-2025-6554	Google	Chromium V8	A Type Confusion in the Google Chromium v8 that enables a remote attacker to perform arbitrary read/write via a crafted HTML page.	Yes	No	Yes	False
CVE-2025-6558	Google	Chromium V8	An Improper Input Validation Vulnerability in the Google Chromium ANGLE and GPU enables remote attackers to perform sandbox escape via a crafted HTML page.	Yes	No	Yes	False
CVE-2025-20281	Cisco	• Identity Services Engine (ISE) • ISE Passive Identity Connector	An Unauthenticated Remote Code Execution Vulnerability in the Cisco ISE and ISE-PIC that enables remote attackers to execute code on the operating system as root.	No	No	Yes	False
CVE-2025-20282	Cisco	• Identity Services Engine (ISE) • ISE Passive Identity Connector	An Arbitrary File Upload Vulnerability in the Cisco ISE and ISE-PIC that enables remote attackers to upload arbitrary files on the operating system as root.	No	No	No	False
CVE-2025-20337	Cisco	• Identity Services Engine (ISE) • ISE Passive Identity Connector	An Unauthenticated Remote Code Execution Vulnerability in the Cisco ISE and ISE-PIC that enables remote	No	No	Yes	False

			attackers to execute code on the operating system as root.				
CVE-2025-25257	Fortinet	FortiWeb	A SQL Injection Vulnerability in the Fortinet FortiWeb that enables an unauthenticated attacker to execute unauthorized SQL code or commands	No	No	Yes	False
CVE-2025-47812	Wing FTP Server	Wing FTP Server	A Remote Code Execution Vulnerability in the Wing FTP Server that enables unauthenticated attackers to perform Lua injection	No	No	Yes	False
CVE-2025-48927	TeleMessage	TM SGNL	An Initialization of a Resource with an Insecure Default Vulnerability in the TeleMessage TM SGNL.	No	No	Yes	False
CVE-2025-48928	TeleMessage	TM SGNL	An Exposure of Core Dump File to an Unauthorized Control Sphere Vulnerability in the TeleMessage TM SGNL.	No	No	Yes	False
CVE-2025-49704	Microsoft	SharePoint	A Code Injection Vulnerability in Microsoft SharePoint that enables authorized attackers to execute code over a network.	No	Yes	Yes	False
CVE-2025-49706	Microsoft	SharePoint	An Improper Authentication Vulnerability in Microsoft SharePoint that enables authorized attackers to perform spoofing over a network.	No	Yes	Yes	False
CVE-2025-53770	Microsoft	SharePoint	An Untrusted Data Vulnerability in the Microsoft SharePoint that enables an unauthorized attacker to execute code over a network.	Yes	Yes	Yes	False
CVE-2025-53771	Microsoft	SharePoint	An Improper Authentication	Yes	Yes	No	False

			Vulnerability in Microsoft SharePoint server that enables unauthorized attackers to perform spoofing over a network.				
CVE-2025-54309	CrushFTP	CrushFTP	An Unprotected Alternate Channel Vulnerability in the CrushFTP allows remote attackers to obtain admin access via HTTPS.	Yes	No	Yes	False
CVE-2023-2533	PaperCut	NG/MF	A Cross-Site Request Forgery Vulnerability in the PaperCut NG/MF that enables an attacker to execute arbitrary code.	No	No	Yes	False
CVE-2019-5418	Rails	Ruby on Rails	A Path Traversal Vulnerability in the Rails Ruby on Rails in Action View.	No	No	Yes	True
CVE-2019-9621	Synacor	Zimbra Collaboration Suite (ZCS)	A Server-Side Request Forgery (SSRF) Vulnerability in the Synacor Zimbra Collaboration Suite (ZCS) via the ProxyServlet component.	No	Yes	Yes	False
CVE-2016-10033	PHP	PHPMailer	A Command Injection Vulnerability in the PHPMailer that enables an attacker to execute arbitrary code within the context of the application.	No	No	Yes	True
CVE-2014-3931	Looking Glass	Multi-Router Looking Glass (MRLG)	A Buffer Overflow Vulnerability in the Multi-Router Looking Glass that enables remote attackers to cause arbitrary memory write and memory corruption.	No	No	Yes	False
CVE-2010-2568	Microsoft	Windows	A Remote Code Execution Vulnerability in Microsoft Windows, if successfully exploited, enables an	No	Yes	Yes	False

			attacker to execute code as the logged-on user				

Ransomware Insights for July

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 July	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.	58	• Education • Healthcare	• CVE-2025-31324 • CVE-2024-21762 • CVE-2024-55591 • CVE-2023-27532
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.	49	• Education • Healthcare • Government sectors	• CVE-2023-3519
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	34	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259

	Kingdom, Canada, Australia, and South Korea. The repercussions are noteworthy, especially within pivotal domains like Services and Goods, Manufacturing, Education, and Finance.			
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.	22	• Government entities • Infrastructure sectors	• CVE-2024-57727 • CVE-2024-57728 • CVE-2024-57726 • CVE-2022-26134
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	19	• Finance • Retail • Real Estate • Manufacture • Construction • Logistic	Unknown

	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.			
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.	16	• Healthcare • Media • Technology • Telecommunication	• CVE-2022-41040 • CVE-2022-41080 • CVE-2022-41082 • CVE-2021-34523 • CVE-2020-12812 • CVE-2018-13379
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	11	• Healthcare • Energy • Manufacturing • Government sector • Education • Defense	Unknown

	ransom demands up to 8 BTC. Handala's operations reflect a mix of ideological hacktivism and disruptive intent, positioning it as a serious threat to critical infrastructure globally			
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.	9	• Education • Finance • Agriculture • Manufacturing • Healthcare • Logistic	Unknown
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	4	• Healthcare • Finance • Technology • Manufacturing	• CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-34362 • CVE-2023-47246 • CVE-2022-2295

	United States, potentially indicating preparations for future attacks.			
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 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.	3	• Education • Healthcare • Manufacturing • Information Technology • Government sectors	• CVE-2020-1472

Conclusion

This month's developments reaffirm the persistent targeting of unpatched enterprise software and critical infrastructure by both ransomware groups and advanced persistent threat actors. The zero-day exploitation, combined with the expanding abuse of secure communication platforms, highlights a pressing need for improved vulnerability management. As threat actors grow more adaptive, organizations must prioritize timely patching, layered defense strategies, and continuous monitoring to stay ahead of evolving risks.

External References:

- https://www.cisa.gov/news-events/alerts/2025/07/22/cisa-adds-four-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/07/10/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/07/02/cisa-adds-one-known-exploited-vulnerability-catalog
- https://thehackernews.com/2025/07/google-patches-critical-zero-day-flaw.html
- https://socprime.com/blog/cve-2025-6558-google-chrome-vulnerability/

- https://securelist.com/the-echo-of-stuxnet-surprising-findings-in-the-windows-exploits-landscape/65367/
- https://www.cisa.gov/news-events/alerts/2025/07/07/cisa-adds-four-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/07/18/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
- https://www.trendmicro.com/en_us/research/23/i/earth-lusca-employs-new-linux-backdoor.html
- https://www.rapid7.com/blog/post/crushftp-zero-day-exploited-in-the-wild/

loginsoft

Connect with us

linkedin.com/loginsoft

x.com/loginsoft_inc

www.loginsoft.com