loginsoft

Monthly Report

Threat & Vulnerabilities Report – June 2025

Executive Summary

As cyber threats grow more sophisticated and rapid in execution, organizations are under constant pressure to minimize patching delays and enhance their defensive posture. In June 2025, the cybersecurity landscape reflected this urgency, with 20 vulnerabilities added to the CISA's Known Exploited Vulnerabilities (KEV) catalog, 7 of which were abused as zero-days.

These exploited flaws affected a broad spectrum of vendors and technologies, from mobile chipsets and CMS platforms to networking gear and operating systems. Notably, vulnerabilities were confirmed in products from Qualcomm, ASUS, Craft CMS, Apple, Microsoft, Google, Linux, D-Link and Fortinet, highlighting the continued targeting of both consumer-facing and enterprise-grade systems by sophisticated threat actors.

Ransomware activity surged this month, with groups such as Qilin, Akira, IncRansom, and DragonForce actively targeting critical sectors. The most affected industries included education, healthcare, government, and manufacturing, highlighting the continued focus of threat actors on organizations with low downtime tolerance and sensitive data.

Actively Exploited Vulnerabilities

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	CISA KEV	OSS
CVE-2025-2783	Google	Chromium Mojo	A Sandbox Escape Vulnerability in the Google Chromium Mojo on Windows arises due to logic error, where an incorrect handle is assigned under certain unspecified conditions.	No	Yes	Yes	False
CVE-2025-3248	Langflow	Langflow	A Missing Authentication Vulnerability in Langflow that enables an unauthenticated remote attacker to execute code via crafted HTTP requests.	No	Yes	Yes	True
CVE-2025-3935	ConnectWise	ScreenConnect	An Improper Authentication Vulnerability in the ConnectWise ScreenConnect enables remote code execution if attackers can obtain and misuse the server's machine keys.	No	No	Yes	False
CVE-2025-4322	Stylemix Themes	Motors theme	An Unauthenticated Privilege Escalation Vulnerability in the Motors theme for WordPress	No	No	No	False

			enables account takeover and the website.				
CVE-2025-5419	Google	Chromium V8	An Out-of-Bounds Read and Write Vulnerability in the Google Chromium V8 that enables remote attackers to potentially exploit heap corruption via a crafted HTML page.	Yes	No	Yes	False
CVE-2025-6543	Citrix	NetScaler ADC/Gateway	A Buffer Overflow Vulnerability in the Citrix NetScaler ADC and NetScaler Gateway that could result in unintended control flow and Denial of Service	Yes	No	Yes	False
CVE-2025-21479	Qualcomm	Multiple Chipsets	An Incorrect Authorization Vulnerability in the graphic component of Qualcomm multiple chipsets.	Yes	No	Yes	False
CVE-2025-21480	Qualcomm	Multiple Chipsets	An Incorrect Authorization Vulnerability in the graphic component of Qualcomm multiple chipsets.	Yes	No	Yes	False
CVE-2025-24016	Wazuh	Wazuh Server	A Deserialization of Untrusted Data Vulnerability in the Wazuh Server that enables remote code execution.	No	Yes	Yes	True
CVE-2025-27038	Qualcomm	Multiple Chipsets	A Use-after-Free Vulnerability in the graphic component of Qualcomm multiple chipsets.	Yes	No	Yes	False
CVE-2025-32433	Erlang	Erlang/OTP	A Missing Authentication for Critical Vulnerability in the Erlang/OTP SSH Server that enables remote code execution.	No	No	Yes	False
CVE-2025-33053	Web Distributed Authoring and Versioning	WebDAV	External Control of File Name or Path Vulnerability in the Web Distributed Authoring and Versioning (WebDAV).	Yes	Yes	Yes	False
CVE-2025-34037	Linksys	Multiple Routers	An OS Command Injection Vulnerability in multiple Linksys routers that enables unauthenticated attackers to inject shell commands	Yes	Yes	No	False
CVE-2025-35939	Craft CMS	Craft CMS	An External Control of Assumed-Immutable Web Parameter Vulnerability in the Craft CMS	No	No	Yes	True

CVE-2025-43200	Apple	Multiple Products	A Zero-click Logic Vulnerability in the Apple multiple products that lead to spyware deployment.	Yes	Yes	Yes	False
CVE-2024-0769	D-Link	DIR-859 Router	A Path Traversal Vulnerability in the D-Link DIR-859 router that can be exploited by remote attackers through a specially crafted input request.	No	No	Yes	False
CVE-2024-3721	TBK	• DVR-4104 • DVR-4216	A Command Injection Vulnerability in the TBK DVR-4104 and DVR-4216 enables attackers to execute system commands without proper authentication.	No	Yes	No	False
CVE-2024-42009	RoundCube	Webmail	A Cross-Site Scripting Vulnerability in the RoundCube Webmail that enables a remote attacker to steal and send emails of a victim via a crafted e-mail message.	No	Yes	Yes	True
CVE-2024-54085	AMI	MegaRAC SPx	An Authentication Bypass by Spoofing Vulnerability in the AMI MegaRAC SPx in the Redfish Host Interface	No	No	Yes	False
CVE-2024-56145	Craft CMS	Craft CMS	A Code Injection Vulnerability in the Craft CMS results in remote code execution on vulnerable systems	No	No	Yes	True
CVE-2023-0386	Linux	Linux Kernel	An Improper Ownership Management Vulnerability in the Linux Kernel that enables a local user to escalate privileges on the system	No	No	Yes	True
CVE-2023-28771	Zyxel	Multiple Firewalls	An OS Command Injection Vulnerability in the Zyxel Multiple Firewalls enables an unauthenticated attacker to execute OS commands remotely by sending crafted packets to an affected device.	No	Yes	Yes	False
CVE-2023-33538	TP-Link	Multiple Routers	A Command Injection Vulnerability in the TP-Link Multiple Routers via the component **/userRpm/WlanNetworkRpm**	No	No	Yes	False

CVE-2023-39780	ASUS	RX-AX55 Routers	An OS Command Injection Vulnerability in the ASUS routers that enables an attacker to execute arbitrary commands on the router	No	Yes	Yes	False
CVE-2021-32030	ASUS	Routers	An Improper Authentication Vulnerability in the ASUS Routers enables an attacker to gain unauthorized access to the administrative interface.	No	Yes	Yes	False
CVE-2019-6693	Fortinet	FortiOS	A Use of Hard-Coded Credentials Vulnerability in the Fortinet FortiOS that enables threat actors to decipher sensitive data.	No	Yes	Yes	False

Ransomware Insights for June

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 June	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.	72	• Education • Healthcare	Unknown
Akira	Akira ransomware underscored a critical security vulnerability linked to the lack of Multi-Factor Authentication (MFA). The nations experiencing the fallout	34	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259

	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.			
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.	26	• Education • Healthcare • Government sectors	CVE-2023-3519
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.	24	• Government entities • Infrastructure sectors	Unknown
Handala	Handala is a politically motivated ransomware group active since late 2023, primarily targeting Israeli organizations across	22	• Healthcare • Energy • Manufacturing • Government sector	Unknown

	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, positioning it as a serious threat to critical infrastructure globally		• Education • Defense	
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.	21	• Healthcare • Media • Technology • Telecommunication	• CVE-2021-34523 • CVE-2022-41080 • CVE-2022-41040 • CVE-2022-41082 • CVE-2018-13379 • CVE-2020-12812
Lynx	Lynx ransomware, active since mid-2024, is a sophisticated malware operating under a	19	• Finance • Retail	Unknown

	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.		• Real Estate • Manufacture • Construction • Logistic	
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	16	• Education • Finance • Agriculture • Manufacturing • Healthcare • Logistic	Unknown

	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.			
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.	4	• Education • Healthcare • Manufacturing • Information Technology • Government sectors	CVE-2020-1472
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	3	• Healthcare • Finance • Technology • Manufacturing	• CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-34362 • CVE-2023-47246 • CVE-2022-2295

	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.			

Conclusion

In conclusion, June 2025 marked a sharp escalation in the global cyber threat landscape, with both newly discovered and legacy vulnerabilities being rapidly weaponized to drive high-impact ransomware campaigns. Critical flaws across widely used technologies including those from Qualcomm, Chromium, and Apple were swiftly integrated into threat actor playbooks, many earning a place on CISA's KEV catalog. This surge in exploitation directly enabled sustained ransomware activity by groups like Qilin, Akira, Inc Ransom, and Play, impacting key sectors such as healthcare, education, finance, and manufacturing. Notably, the emergence of Handala ransomware signaled a concerning trend toward ideologically motivated attacks that blur the lines between cybercrime and cyber warfare. As ransomware operations become increasingly exploit-driven and strategic, organizations must prioritize rapid patching, infrastructure hardening, and threat visibility to stay ahead of evolving adversaries.

External References:

- https://www.cisa.gov/news-events/alerts/2025/06/02/cisa-adds-five-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/06/03/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/06/05/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/06/09/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/06/16/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/06/17/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/06/25/cisa-adds-three-known-exploited-vulnerabilities-catalog

- https://www.cisa.gov/news-events/alerts/2023/05/31/cisa-adds-one-known-exploited-vulnerability-catalog
- https://blog.qualys.com/vulnerabilities-threat-research/2024/10/02/threat-brief-understanding-akira-ransomware
- https://blog.sekoia.io/vicioustrap-infiltrate-control-lure-turning-edge-devices-into-honeypots-en-masse/
- https://www.greynoise.io/blog/exploit-attempts-targeting-zyxel-cve-2023-28771
- https://securelist.com/mirai-botnet-variant-targets-dvr-devices-with-cve-2024-3721/116742/
- https://www.trendmicro.com/en_us/research/25/f/langflow-vulnerability-flodric-botnet.html
- https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/team46-and-taxoff-two-sides-of-the-same-coin