Monthly Report

loginsoft

Threat & Vulnerabilities Report - August 2024

Executive Summary

August 2024 has been a critical month in cybersecurity, marked by the addition of 19 new vulnerabilities to the CISA Known Exploited Vulnerabilities (KEV) list, with eight impacting Microsoft Windows. This highlights a significant challenge for Microsoft, as both newly discovered and older vulnerabilities in Windows are being actively exploited, underscoring the need for stronger security measures.

Google Chrome also faced serious security issues this month, with two vulnerabilities, **CVE-2024-7965** and **CVE-2024-7971** being actively exploited as zero-days. These incidents raise the total number of zero-day vulnerabilities addressed by Google in 2024 to ten, reflecting persistent concerns about browser security.

The Mirai botnet has escalated its activities, targeting vulnerabilities in Avtech security cameras and Apache OFBiz. In parallel, advanced threat actors like APT 41, Volt Typhoon, Intel Broker, APT-C-60, UNC 5174, and SideWinder have been highly active, adding complexity to the threat landscape.

Additionally, there has been a spike in attacks on VMware ESXi hypervisors, with groups like Storm-1175, Storm-0506, and Octo Tempest exploiting **CVE-2024-37085** to deploy ransomware strains including Akira, BlackBasta, BlackByte, and LockBit. Simultaneously, Sysrv Botnet, XMRig, and Cerber ransomware have been exploiting an older vulnerability in Atlassian Confluence Data servers.

Actively Exploited Vulnerabilities

CVE-ID	Affected Product	Severity	Description	Zero-day	Actively Exploited	Abused by Malware	CISA KEV	OSS
CVE-2024-7971	Google Chrome	High	A type confusion bug in the V8 JavaScript and WebAsembly engine that can enable a remote attacker to exploit heap corruption via a crafted HTML page.	Yes	Yes	Yes	Yes	Yes
CVE-2024-7965	Google Chrome	High	An inappropriate implementation bug in the V8 JavaScript and WebAssembly engine that could enable a remote attacker to potentially exploit heap corruption via a crafted HTML page.	Yes	Yes	No	Yes	No
CVE-2024-28000	LiteSpeed Cache WordPress plugin	Critical	An unauthenticated privilege escalation vulnerability in the LiteSpeed Cache WordPress plugin that allows unauthenticated attackers to escalate their privileges and gain administrative access on the affected sites	No	Yes	No	No	No

CVE-2024-36971	Android Kernel	High	A use after free vulnerability in the Linux kernel network routing component. Requiring elevated privileges, this flaw can be exploited to manipulate network traffic behavior.	Yes	Yes	Yes	Yes	Yes
CVE-2024-39717	Versa Director GUI	High	A file upload vulnerability impacting the "Change Favicon" feature that allows threat actor to upload malicious files disguised as harmless PNG images.	Yes	Yes	Yes	Yes	False
CVE-2024-7029	Avtech Security cameras	High	A command injection vulnerability in the Avtech Security cameras that could be leveraged by the attacker to inject commands over the network and execute them without any authentication requirement.	No	Yes	Yes	No	False
CVE-2024-38856	Apache OFBiz	Critical	An incorrect authorization vulnerability in the Apache OFBiz, that can be exploited by remote and unauthenticated attackers to execute arbitrary code on vulnerable systems.	Yes	Yes	No	Yes	False
CVE-2024-32113	Apache OFBiz	Critical	A path traversal vulnerability in the Apache OFBiz that can potentially lead to remote code execution.	No	Yes	Yes	Yes	No
CVE-2024-4885	Progress WhatsUp Gold	Critical	A remote code execution vulnerability in the Progress WhatsUp Gold that can allow attackers to execute arbitrary code remotely without requiring any authentication.	No	Yes	Yes	No	No
CVE-2024-28986	SolarWinds Web Help Desk	Critical	Deserialization of Untrusted Data vulnerability in SolarWinds	No	Yes	No	Yes	No

			Web Help Desk through 12.8.3 leads to remote code execution.					
CVE-2024-37085	VMware ESXi hypervisor	High	An Active Directory integration authentication bypass vulnerability in the VMware ESXi supervisors which can result in the attacker taking complete control of the affected system.	Yes	Yes	Yes	Yes	No
CVE-2024-38107	Windows Power Dependency Coordinator	High	Use After Free vulnerability in Windows Power Dependency Coordinator leads to privilege escalation	Yes	Yes	No	Yes	No
CVE-2024-38193	Windows Ancillary Function Driver	High	Use After Free vulnerability in Windows Ancillary Function Driver for WinSock leads to privilege escalation	Yes	Yes	No	Yes	No
CVE-2024-38106	Microsoft Windows Kernel	High	Privilege Escalation vulnerability in Microsoft Windows Kernel	Yes	Yes	No	Yes	No
CVE-2024-38189	Microsoft Project	High	Remote Code Execution vulnerability in Microsoft Project	Yes	Yes	No	Yes	No
CVE-2024-38178	Windows Scripting Engine	High	Memory Corruption vulnerability in Windows Scripting Engine leads to remote code execution	Yes	Yes	No	Yes	No
CVE-2024-38213	Microsoft Windows SmartScreen	Medium	Security Feature Bypass vulnerability in Microsoft Windows SmartScreen.	Yes	Yes	No	Yes	No
CVE-2024-23897	Jenkins Command Line Interface (CLI)	Critical	A path traversal vulnerability in the Jenkins Command Line Interface (CLI) that could potentially lead to code execution.	No	Yes	Yes	Yes	Yes

CVE-2024-7262	WPS Office	High	An improper path validation vulnerability in the Kingsoft WPS Office, that could allow attackers to execute arbitrary code on a user's system.	No	Yes	Yes	No	No
CVE-2023-22527	Confluence Data Center and Confluence Server	Critical	A template injection vulnerability found in the older versions of Confluence Data Center and Server that enables unauthenticated attacker to achieve remote code execution on the vulnerable systems.	No	Yes	Yes	Yes	False
CVE-2022-0185	Linux Kernel	High	A heap-based buffer overflow vulnerability in the Filesystem Context functionality of Linux Kernel that enables an attacker to gain elevated privileges on the affected systems.	No	Yes	Yes	Yes	Yes
CVE-2021-33044	Dahua IP camera	Critical	Authentication bypass vulnerability in the Dahua IP cameras that can be exploited remotely during login process by sending specially crafted data packets to the target system.	No	Yes	No	Yes	No
CVE-2021-33045	Dahua IP camera	Critical	Authentication bypass vulnerability in the Dahua IP cameras that can be exploited remotely during login process by sending specially crafted data packets to the target system.	No	Yes	No	Yes	No
CVE-2021-31196	Microsoft Windows Exchange Server	High	A remote code execution vulnerability in the Microsoft Exchange Server that can be leveraged by an attacker to execute arbitrary	No	Yes	No	Yes	No

			codes on the affected server.					
CVE-2018-0824	Microsoft Windows	High	A deserialization of untrusted data vulnerability in Microsoft COM for Windows which can lead to remote code execution.	No	Yes	Yes	Yes	No
CVE-2017-0199	Microsoft Office and WordPad	High	A remote code execution vulnerability in Microsoft Office and WordPad that can be leveraged by an attacker to take complete control of the affected system.	No	Yes	Yes	Yes	No
CVE-2017-11882	Microsoft Office	High	A memory corruption vulnerability in Microsoft Office allows attackers to execute malicious code by exploiting the software's improper handling of in-memory data.	No	Yes	Yes	Yes	No

Ransomware Insights

The following table presents the top 10 ransomware strains from August, detailing the number of affected organizations. It also lists associated CVEs linked to these ransomware strains, regardless of when those vulnerabilities were actually exploited.

Ransomware	Description	No. of Affected Organizations for August Month	Targeted Industries	Vulnerabilities Abused Most
Ransomhub	Ransomhub is a self-described Ransomware-as-a-Service operation first disclosed in announcements on the Russian-language dark web forum RAMP in February 2024. The encryptor has versions written in C++ and the Go programming language and claims to support encryption of Windows, Linux, and ESXi devices. Initial posts announcing the group explicitly forbid attacks on the Commonwealth of Independent States, Cuba, North Korea, and China, as well as encryption of non-profit hospitals. At the time of this report, Ransomhub has publicly claimed five distinct organizations across nine posts from February 10th to March 4th on its data leak site	54	• Education • Construction • Government	• CVE-2020-1472

Meow	Meow ransomware, a modified version of Conti-2 Ransomware, encrypts data on compromised servers using the ChaCha20 algorithm and demands ransom payment instructions via email or Telegram. The ransomware's note is marked by the phrase "MEOW! MEOW! MEOW!" and logins repeating "meowcorp2022." Discovered in late 2022 as one of four strains derived from Conti's leaked code, Meow ransomware operated from August 2022 to February 2023. In March 2023, a free decryptor was released, leading to a cessation of activity. However, the Meow group remains active in 2024, with nine victims reported so far, including three in March, targeting significant institutions.	36	• Healthcare • Finance • Education • Government • Manufacturing	• Unknown
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.	29	• Healthcare • Media • Technology • Telecommunication	• CVE-2021-34523 • CVE-2022-41080 • CVE-2022-41040 • CVE-2022-41082 • CVE-2018-13379 • CVE-2020-12812
Hunters	Hunters International, identified as a Ransomware-as-a-Service (RaaS) provider, emerged after the detection of source code sharing resemblances with the infamous Hive ransomware strain. Initial examination of the malware code revealed an estimated 60% similarity with samples from Hive ransomware version 61. Detailed technical analysis proposes a plausible scenario in which the ransomware could have been employed in activities associated with the recently dismantled Hive cartel.	17	• Healthcare • Education • Research	• 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	16	• Education • Healthcare • Manufacturing • Information Technology	• CVE-2020-1472

	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.		• Government sectors	
Lockbit3	Operating since 2019, LockBit ransomware, previously known as ABCD, originated from the Megacortex family and spread through diverse channels such as RDP attacks, phishing, and exploiting public-facing applications. The most recent version, LockBit 3.0, functions as a ransomware-as-a-service model.	16	• Education • Healthcare • Technology • Manufacture • Utilities • Construction • Entertainment	• CVE-2023-40044 • CVE-2023-4966 • CVE-2023-20269 • CVE-2023-27350 • CVE-2023-27351 • CVE-2022-36537 • CVE-2022-41082 • CVE-2024-1708 • CVE-2024-1709
Bianlian	BianLian is a Golang-based ransomware that significantly threatens diverse industries, including healthcare, education and government entities. Recognizing the severity of this threat, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and Australian Cyber Security Centre (ACSC) have collaboratively issued advisories, emphasizing the group's focus on critical infrastructure sectors in the United States and Australia. Upon infiltrating systems, the BianLian group adeptly utilizes open-source tools and command-line scripts to extract victims' data to a cloud storage controlled by attackers. Initially adopting a double-extortion model, the group shifted its strategy towards data exfiltration attacks after releasing a free decryptor.	15	• Healthcare • Banking • Utilities • Insurance	• CVE-2023-27350 • CVE-2022-37042 • CVE-2022-27925 • CVE-2021-4034 • CVE-2021-34523 • CVE-2021-34473 • CVE-2021-31207
Blacksuit	BlackSuit ransomware, a rebranded version of the infamous Royal ransomware, emerged in May 2023 following intensified law enforcement actions. This strategic rebranding allows the group to evade detection and continue its cybercriminal activities. Originating from the remnants of the Conti group, BlackSuit targets high-profile sectors, including healthcare, education, IT, government, retail, and manufacturing, while excluding entities in the Commonwealth of Independent States (CIS). Both large enterprises and SMBs are	11	• Information technology • Government • Retail • Manufacturing	Unknown

	at risk from this private ransomware/extortion operation			
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.	10	• Education • Healthcare	• CVE-2023-40044 • CVE-2023-4966 • CVE-2023-20269 • CVE-2023-27350 • CVE-2023-27351 • CVE-2022-36537 • CVE-2022-41082
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.	9	• Education • Healthcare • Government sectors	• CVE-2023-3519

Conclusion

August 2024 has been a critical month for addressing high-severity vulnerabilities across multiple platforms and applications. Tech giants Google and Microsoft faced significant security challenges, as most vulnerabilities added to the CISA KEV list targeted their products. The escalation in Mirai botnet attacks and the surge in ransomware attacks on VMware ESXi hypervisors highlight a broader trend of sophisticated and aggressive exploitation tactics. The active involvement of threat actors like APT 41 and Volt Typhoon underscores the urgent need for strengthened cybersecurity measures. These developments emphasize the critical importance of proactive security strategies, timely updates, and continuous monitoring to defend against persistent and evolving threats. Organizations must remain vigilant and responsive to protect their systems and data in an increasingly complex threat landscape.

Sources Cited:

1. https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/
2. https://www.cisa.gov/news-events/alerts/2024/08/26/cisa-adds-one-known-exploited-vulnerability-catalog
3. https://www.cisa.gov/news-events/alerts/2024/08/28/cisa-adds-one-known-exploited-vulnerability-catalog
4. https://vulert.com/blog/android-kernel-vulnerability-patch/
5. https://www.cisa.gov/news-events/alerts/2024/08/07/cisa-adds-two-known-exploited-vulnerabilities-catalog
6. https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/

7. https://www.akamai.com/blog/security-research/2024-corona-mirai-botnet-infects-zero-day-sirt
8. https://www.cisa.gov/news-events/alerts/2024/08/27/cisa-adds-one-known-exploited-vulnerability-catalog
9. https://www.microsoft.com/en-us/security/blog/2024/08/08/chained-for-attack-openvpn-vulnerabilities-discovered-leading-to-rce-and-lpe/
10. https://blog.talosintelligence.com/blackbyte-blends-tried-and-true-tradecraft-with-newly-disclosed-vulnerabilities-to-support-ongoing-attacks/
11. https://www.cisa.gov/news-events/alerts/2024/08/13/cisa-adds-six-known-exploited-vulnerabilities-catalog
12. https://www.cloudsek.com/blog/born-group-supply-chain-breach-in-depth-analysis-of-intelbrokers-jenkins-exploitation
13. https://www.cisa.gov/news-events/alerts/2024/08/05/cisa-adds-one-known-exploited-vulnerability-catalog
14. https://www.cisa.gov/news-events/alerts/2024/08/21/cisa-adds-four-known-exploited-vulnerabilities-catalog
15. https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect
16. https://blogs.blackberry.com/en/2024/07/sidewinder-targets-ports-and-maritime-facilities-in-the-mediterranean-sea
17. https://blog.talosintelligence.com/chinese-hacking-group-apt41-compromised-taiwanese-government-affiliated-research-institute-with-shadowpad-and-cobaltstrike-2/
18. https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect
19. https://www.trendmicro.com/en_ph/research/24/h/cve-2023-22527-cryptomining.html
20. https://www.welivesecurity.com/en/eset-research/analysis-of-two-arbitrary-code-execution-vulnerabilities-affecting-wps-office/

loginsoft

Connect with us

linkedin.com/loginsoft

x.com/loginsoft

www.loginsoft.com