Monthly Report

loginsoft

Threat & Vulnerabilities Report - July 2024

Executive Summary

This month, 14 new CVEs were added to the CISA KEV (Known Exploited Vulnerabilities) list, with three specifically impacting Microsoft Windows products. Alarmingly, older vulnerabilities continue to cause major disruptions, as several CVEs from last year remain actively exploited in the wild.

One notable case involves unauthenticated access to the Twilio Authy API, allowing attackers to disclose phone numbers. Additionally, a chained attack leveraging three distinct vulnerabilities within ServiceNow instances has enabled remote code execution (RCE), posing a serious risk of data exfiltration.

On the botnet front, Reaper, Zerobot, and Sysrv have been observed exploiting IoT devices, routers, and Apache HTTP servers to gain control and conduct malicious activities. VMware is the latest high-profile target, as a newly discovered and easy-to-exploit vulnerability in its ESXi platform has opened the door for attackers to gain full control of the host, has quickly become a favored tool among ransomware groups, with multiple attacks already reported exploiting this flaw.

Actively Exploited Vulnerabilities

CVE-ID	Affected Product	Severity	Description	Zero-day	Actively Exploited	Abused by Malware	CISA KEV	OSS
CVE-2024-20399	Cisco NX-OS Software	Medium	A vulnerability in Cisco NX-OS allows an authenticated user with administrative privileges to execute arbitrary commands with root-level access by manipulating input within specific CLI commands.	No	Yes	Yes	Yes	False
CVE-2024-23692	Rejetto HTTP File Server (HFS)	Critical	A critical flaw in Rejetto HTTP File Server enables remote attackers to execute malicious commands on the system by submitting specially crafted HTTP requests.	No	Yes	Yes	Yes	False
CVE-2024-39891	Twilio Authy API	Medium	Twilio's Authy API contained a vulnerability that allowed anyone to check if a phone number was registered for Authy without authentication.	No	Yes	Yes	Yes	False
CVE-2024-6387	OpenSSH	High	A flaw in OpenSSH allows attackers to gain unrestricted root access to vulnerable Linux systems without requiring any authentication. This vulnerability arises from a timing-based attack that exploits a race condition in the OpenSSH server.	No	Yes	Yes	No	True
CVE-2024-38080	Windows Hyper-V	High	A vulnerability in Microsoft Windows Hyper-V allows attackers to bypass user	Yes	Yes	No	Yes	False

			restrictions and gain unrestricted system-level access.					
CVE-2024-38112	Windows MSHTML Platform	High	A vulnerability in Windows MSHTML allows attackers to disguise malicious content as legitimate content by embedding it within a specially crafted HTML file..	Yes	Yes	Yes	Yes	False
CVE-2024-29510	Artifex Ghostscript	Medium	A vulnerability in Artifex Ghostscript allows attackers to bypass security restrictions by injecting malicious code through format string manipulation.	No	Yes	No	No	True
CVE-2024-5441	Modern Events Calendar plugin for WordPress	High	The Modern Events Calendar plugin allows attackers to upload harmful files to a WordPress website, potentially leading to a site takeover.	No	Yes	No	No	Fasle
CVE-2024-36401	OSGeo's GeoServer and GeoTools	Critical	A flaw in GeoServer allows attackers to execute malicious code remotely by manipulating data input.	No	Yes	No	Yes	True
CVE-2024-28995	SolarWinds Serv-U	High	A flaw in SolarWinds Serv-U allows unauthorized users to access and view sensitive files on the server.	No	Yes	Yes	Yes	False
CVE-2024-34102	Adobe Commerce	Critical	A critical vulnerability in Adobe Commerce and Magento allows attackers to execute malicious code by exploiting improper handling of XML data, potentially leading to a complete system takeover.	No	Yes	No	Yes	True
CVE-2024-4879	ServiceNow 's Now Platform	Critical	A critical flaw in ServiceNow's UI Macros allows anyone to execute malicious code within the platform without requiring any login.	No	Yes	No	Yes	False
CVE-2024-37085	VMware ESXi hypervisors	Medium	A flaw in VMware ESXi's Active Directory integration allowed attackers to bypass authentication and gain complete control of the system.	Yes	Yes	Yes	No	False
CVE-2023-28252	Windows Common Log File System Driver	High	A flaw in Windows allows users with limited privileges to escalate their access to the highest level of system control.	No	Yes	Yes	Yes	False

CVE-2023-45249	Acronis Cyber Infrastructure (ACI)	Critical	Acronis Cyber Infrastructure (ACI) contained a critical flaw that allowed attackers to bypass security measures and gain complete control of the system by exploiting default passwords.	No	Yes	No	Yes	False
CVE-2022-22948	vCenter Server	Medium	A security flaw in VMware vCenter allows unauthorized access to sensitive information due to improper file protection.	No	Yes	Yes	Yes	False
CVE-2012-4792	Microsoft Internet Explorer	High	A Use-after-free vulnerability in the Microsoft Internet Explorer which, when successfully exploited, allows an attacker to execute malicious commands on the affected systems.	No	Yes	Yes	Yes	False

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
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	38	• Education • Construction • Government	• CVE-2020-1472

	publicly claimed five distinct organizations across nine posts from February 10th to March 4th on its data leak site			
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.	33	• 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
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.	25	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259
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.	24	• Healthcare • Education • Research	Unknown
Play	The Play ransomware group, also identified as Balloonfly and PlayCrypt, has	21	• Healthcare • Media	• CVE-2021-34523 • CVE-2022-41080

	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.		• Technology • Telecommunication	• CVE-2022-41040 • CVE-2022-41082 • CVE-2018-13379 • CVE-2020-12812
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.	17	• Healthcare • Finance • Technology • Manufacturing	• CVE-2022-2295 • CVE-2023-34362 • CVE-2023-47246 • CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351
Inc Ransom	Inc. ransomware, which emerged in June 2023, spread through spear-phishing emails and targeted vulnerable	12	• Education • Healthcare • Government sectors	• CVE-2023-3519

	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.			
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 at risk from this private ransomware/extortion operation	11	• Information technology • Government • Retail • Manufacturing	Unknown
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	11	• 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

	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.			
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.	10	• Education • Healthcare • Manufacturing • Information Technology • Government sectors	CVE-2020-1472
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	8	• Education • Healthcare	• CVE-2023-40044 • CVE-2023-4966 • CVE-2023-20269 • CVE-2023-27350 • CVE-2023-27351 • CVE-2022-36537 • CVE-2022-41082

	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.			
BlackBasta	Black Basta is a ransomware group operating as ransomware-as-a-service (RaaS) that was initially spotted in April 2022. It has since proven itself to be a formidable threat, as evidenced by its use of double-extortion tactics and expansion of its attack arsenal to include tools like the Qakbot trojan and PrintNightmare exploit.	7	• Technology • Insurance • Manufacturing • Utilities • Real estate • Finance	• CVE-2019-16098 • CVE-2021-42278 • CVE-2020-1472 • CVE-2021-34527 • CVE-2019-16098 • CVE-2021-42287

Dispossessor	Dispossessor ransomware is an active threat targeting victims with encryption-based attacks to extort ransom payments. It operates similarly to other ransomware groups, such as LockBit. Dispossessor gained attention due to its strikingly similar website and potential affiliation with LockBit or impersonation. Affiliates of Dispossessor have unlimited access and operate globally, showcasing its broad reach and potentially international impact. While decryption tools for Dispossessor exist, victims may still face significant risks and data loss. The ransomware ecosystem continues to evolve, with data leak site operators like RansomHub and Dispossessor contributing to new extortion cycles	5	• Healthcare • Financial Services • Government • Manufacturing • Education	Unknown
cactus	Active since March 2023, Cactus ransomware has primarily focused on U.S. manufacturing companies by exploiting vulnerabilities in VPN appliances to initiate unauthorized access. More than 80 victims, including high-profile targets, were victims of this ransomware. Notably, the ransomware exhibits unique evasion techniques, such as encrypting the malware binary to evade anti-malware detection.	2	• commercial entities • Lawfirms • Manufacturing	• CVE-2023-41265 • CVE-2023-41266 • CVE-2023-48365

Conclusion

Considering the recent additions to the CISA KEV list and the ongoing exploitation of both old and new vulnerabilities, it is evident that the cyber threat landscape remains highly dynamic and perilous. The continued targeting of outdated CVEs alongside newly discovered flaws, such as those in VMware's ESXi and ServiceNow, demonstrates that attackers are constantly evolving their tactics, finding opportunities in even seemingly well-established systems. The rise of botnets like Reaper and Zerobot further emphasizes the growing risks faced by IoT devices, routers, and servers. Organizations must adopt a proactive approach to vulnerability management, ensuring that patches are applied promptly, threat intelligence is continuously updated, and robust defense mechanisms are in place.

External References:

1. https://www.greynoise.io/blog/perma-vuln-d-link-dir-859-cve-2024-0769
2. https://www.cisa.gov/news-events/alerts/2024/07/02/cisa-adds-one-known-exploited-vulnerability-catalog
3. https://www.trendmicro.com/en_us/research/21/i/remote-code-execution-zero-day--cve-2021-40444--hits-windows--tr.html
4. https://www.fortinet.com/blog/threat-research/merkspy-exploiting-cve-2021-40444-to-infiltrate-systems
5. https://unit42.paloaltonetworks.com/threat-brief-cve-2024-6387-openssh/
6. https://www.qualys.com/regresshion-cve-2024-6387/
7. https://www.cisa.gov/news-events/alerts/2024/02/13/cisa-adds-two-known-exploited-vulnerabilities-catalog
8. https://www.trendmicro.com/en_in/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html
9. https://www.cisa.gov/news-events/alerts/2024/07/17/cisa-adds-three-known-exploited-vulnerabilities-catalog
10. https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations
11. https://sansec.io/research/cosmicsting
12. https://securityonline.info/docker-users-beware-cve-2024-41110-cvss-10-could-lead-to-system-takeover/
13. https://arcticwolf.com/resources/blog/cve-2024-4879-cve-2024-5178-cve-2024-5217/
14. https://www.assetnote.io/resources/research/chaining-three-bugs-to-access-all-your-servicenow-data
15. https://www.cisa.gov/news-events/alerts/2024/07/29/cisa-adds-three-known-exploited-vulnerabilities-catalog
16. https://www.cisa.gov/news-events/alerts/2024/07/30/cisa-adds-one-known-exploited-vulnerability-catalog
17. https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/