loginsoft

Monthly Report

Threat & Vulnerabilities Report – October 2024

Executive Summary

October 2024 saw a slight dip in the number of vulnerabilities added to the CISA Known Exploited Vulnerabilities list, with only 17 new entries compared to the previous month's 26. However, all these 17 vulnerabilities were newly discovered in 2024, highlighting the ongoing threat landscape.

Microsoft and Ivanti remained in focus as top targets, with four and three vulnerabilities added to the CISA KEV list, respectively, alongside two vulnerabilities from Fortinet, reflecting the persistent threat landscape. In addition, prominent tech giants Qualcomm, Mozilla, and Cisco reported one vulnerability added to the CISA KEV list.

Recent cyber threat activity has highlighted a range of actors exploiting critical vulnerabilities across multiple platforms. The Earth Simnavaz group (APT34) leveraged a Windows kernel privilege escalation flaw, while UNC5820 exploited a vulnerability in Fortinet FortiManager. LemonDuck malware also targeted an older Microsoft vulnerability, and Veeam Backup & Replication was exploited alongside attacks by the Akira and Fog ransomware groups.

Additionally, threat actors exploited three critical remote code execution vulnerabilities (**CVE-2024-51567**, **CVE-2024-51568** and **CVE-2024-51378**) in CyberPanel to deploy PSAUX ransomware, and the latest LightSpy malware variant used two iOS exploits (**CVE-2020- 9802** and **CVE-2020-3837**) for initial access and privilege escalation. These developments underscore the urgent need for reinforced, cross-platform security measures to address the evolving threat landscape.

Actively Exploited Vulnerabilities

CVE-ID	Affected Product	Severity	Description	Zero -day	Actively Exploited	Abused by malware	CISA KEV	OSS
CVE-2024-29824	Ivanti Endpoint Manager (EPM)	Critical	A SQL injection vulnerability in Ivanti EPM allows unauthenticated attackers within the same network to execute malicious code on unpatched systems.	No	Yes	No	Yes	False
CVE-2024-45519	Zimbra Collaboration	Critical	A remote code execution vulnerability in Zimbra's postjoural service that could enable unauthenticated threat actors to execute arbitrary commands on the vulnerable systems.	No	Yes	No	Yes	False
CVE-2024-43047	Qualcomm Multiple Chipsets	High	A use after free vulnerability in the Qualcomm Digital	Yes	Yes	No	Yes	False

			Signal Processor (DSP) service.					
CVE-2024-43572	Microsoft Management Console	High	A remote code execution vulnerability in Microsoft Management Console (MMC) that can be exploited by tricking users into opening a malicious file, often through social engineering techniques.	Yes	Yes	No	Yes	False
CVE-2024-43573	Microsoft Windows MSHTML Platform	Medium	A spoofing vulnerability in the Windows MSHTML Platform	Yes	Yes	No	Yes	False
CVE-2024-9379	Ivanti Cloud Service Appliance	Medium	A SQL injection vulnerability in the Ivanti CSA admin web console allows a remote, authenticated attacker with administrator privileges to execute arbitrary SQL commands.	Yes	Yes	No	Yes	False
CVE-2024-9380	Ivanti Cloud Service Appliance	High	A command injection vulnerability in the Ivanti CSA admin web console could allow a remote, authenticated attacker with administrator privileges to execute arbitrary commands on the system.	Yes	Yes	No	Yes	False
CVE-2024-9381	Ivanti Cloud Service Appliance	High	A path traversal vulnerability in Ivanti CSA could allow a remote, authenticated attacker with administrator privileges to bypass security restrictions.	Yes	Yes	No	No	False
CVE-2024-23113	Fortinet FortiOS	Critical	A critical remote code execution vulnerability	No	Yes	No	Yes	False

			in Fortinet FortiOS allows unauthenticated attackers to execute commands on vulnerable devices without requiring any user interaction.					
CVE-2024-30088	Windows Kernel	High	A privilege escalation vulnerability in the Windows kernel could allow attackers to elevate their privileges to SYSTEM level, granting them significant control over compromised devices.	No	Yes	Yes	Yes	False
CVE-2024-9680	Mozilla Firefox	Critical	A use-after-free vulnerability in the Animation timeline component of Mozilla Firefox.	No	Yes	No	Yes	False
CVE-2024-28987	SolarWinds Web Help Desk (WHD)	Critical	A critical hardcoded credential vulnerability in the SolarWinds Web Help Desk (WHD) software that enables remote unauthenticated users to access internal functionality and modify data.	No	Yes	No	Yes	False
CVE-2024-40711	Veeam Backup & Replication	Critical	A deserialization of untrusted data vulnerability in Veeam Backup & Replication that allows for unauthenticated remote code execution	No	Yes	Yes	Yes	False
CVE-2024-38178	Microsoft Internet Explorer (IE)	High	A memory corruption vulnerability in the scripting engine that could lead to remote code execution when using the Edge browser in Internet Explorer mode.	Yes	Yes	Yes	Yes	False

CVE-2024-44133	macOS	Medium	A vulnerability in macOS, referred to as "HM Surf," enables attackers to circumvent the operating system's Transparency, Consent, and Control (TCC) technology, allowing them unauthorized access to a user's protected data.	No	Yes	Yes	No	False
CVE-2024-9537	ScienceLogic SL1	Critical	A remote code execution vulnerability in the ScienceLogic SL1 platform could allow unauthorized access to its internal performance reporting systems.	Yes	Yes	Yes	Yes	False
CVE-2024-37383	Roundcube Webmail	Medium	A stored cross-site scripting (XSS) vulnerability has been identified in Roundcube Webmail, which can be exploited via SVG animate attributes.	No	Yes	Yes	Yes	True
CVE-2024-38094	Microsoft SharePoint server	High	A deserialization vulnerability in Microsoft SharePoint allows attackers to potentially execute arbitrary commands on affected systems.	No	Yes	No	Yes	False
CVE-2024-44068	Samsung Mobile Processor	High	A use-after-free vulnerability in the Samsung Mobile Processor that can lead to privilege escalation	No	Yes	No	No	False
CVE-2024-20481	Cisco ASA and Cisco FTD	Medium	A vulnerability in the Remote Access VPN (RAVPN) service of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could enable an unauthenticated	No	Yes	No	Yes	False

			remote attacker to trigger a denial-ofservice (DoS) attac					
CVE-2024-47575	Fortinet FortiManager	Critical	A missing authentication vulnerability in the Fortinet FortiManager fgfmd daemon could allow a remote, unauthenticated attacker to execute arbitrary code or commands by sending specially crafted requests	No	Yes	Yes	Yes	False
CVE-2017-0144	Microsoft's Server Message Block (SMB) protocol	High	A remote code execution vulnerability in the Microsoft Server Message Block (SMB) server could be exploited by an attacker to execute arbitrary code on a targeted server, potentially granting them control over the system	No	Yes	Yes	Yes	False

Ransomware Insights for October

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 October 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	79	• Education • Construction • Government	CVE-2020-1472

	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			
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.	53	• Healthcare • Media • Technology • Telecommunication	• CVE-2021-34523 • CVE-2022-41080 • CVE-2022-41040 • CVE-2022-41082 • CVE-2018-13379 • CVE-2020-12812
Meow	Meow ransomware, a modified version of Conti-2 Ransomware, encrypts data on compromised servers using the ChaCha20 algorithm and demands ransom	24		

	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.		• Healthcare • Finance • Education • Government • Manufacturing	Unknown
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.	23	• Healthcare • Education • Research	Unknown
FOG	Fog ransomware, emerging in May 2024, initially targeted educational and recreational sectors by exploiting compromised VPN credentials to infiltrate systems. More recently, the group has shifted focus toward high-revenue sectors like financial services, broadening its victim base and refining tactics to maximize ransom potential. This	23	• Education • Recreation	• CVE-2024-40711 • CVE-2024-40766

	adaptive approach underscores Fog ransomware's escalating threat, as it increasingly prioritizes industries where operational disruption could drive substantial ransom demands.			
ElDorado	The Eldorado ransomware is a sophisticated Ransomware-as-a-Service (RaaS) operation that targets both Windows and Linux environments, specifically aiming at VMware ESXi systems and virtual machines (VMs). Developed using the Golang programming language, this ransomware is designed for cross-platform functionality, enabling attacks across multiple operating systems and broadening its reach. Eldorado operates through dedicated leak sites (DLS) on the dark web, where it advertises stolen data and threatens to release it publicly if ransoms are not paid.	20	• Healthcare • Financial • Government Agencies • Manufacturing • Industrial Sectors • Telecommunications	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 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
Qilin	The Qilin ransomware has been in existence since August 2022, also recognized as Agenda, has posed a	14		

	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.		• Education • Healthcare	• CVE-2023-40044 • CVE-2023-4966 • CVE-2023-20269 • CVE-2023-27350 • CVE-2023-27351 • CVE-2022-36537 • CVE-2022-41082
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.	13	• Information technology • Government • Retail • Manufacturing	Unknown
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.	10	• Technology • Insurance • Manufacturing • Utilities • Real estate • Finance	• CVE-2021-42278 • CVE-2020-1472 • CVE-2021-34527 • CVE-2019-16098 • CVE-2021-42287
Akira	Akira ransomware underscored a critical security vulnerability linked to the lack of Multi-Factor Authentication (MFA). The nations	10		

	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.		• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259
Raworld	RA World ransomware is a sophisticated threat that employs multistage components and anti-antivirus (AV) tactics to ensure maximum impact on its victims. The ransom note delivered by RA World informs victims that their files have been encrypted and stolen, listing the types of data exfiltrated, which indicates a double extortion tactic where victims are coerced into paying to prevent data leaks in addition to decrypting their files. RA World has been reported to hold over 20 organizations worldwide hostage for financial gains, showcasing its broad reach and the severity of its attacks. Specifically targeting sectors such as healthcare, insurance, and financial services, RA World operators breach systems through compromised domain credentials, illustrating a focused approach on industries where data sensitivity and uptime are critical. The ransomware variant appends a .RAWLD extension to encrypted files, marking them as inaccessible without the decryption key provided by the attackers upon ransom payment. Additionally, RA World has shown a particular focus on healthcare organizations in the	9	• Healthcare • Finance • Insurance	Unknown

	Latin American region, indicating a geographic as well as sector-based specificity in its targeting strategy.			

Conclusion

October 2024 underscored an evolving threat landscape with 17 new vulnerabilities added to the CISA Known Exploited Vulnerabilities list, signaling ongoing risks despite fewer additions than the previous month. Key vendors like Microsoft, Ivanti, and Fortinet faced targeted attacks, highlighting cybercriminals' focus on widely used platforms. The active exploitation by APT groups and ransomware operators across diverse systems, from Windows to CyberPanel, emphasizes the urgent need for organizations to enhance cross-platform security measures and implement rapid vulnerability management to protect against increasingly sophisticated threats.

External References

1. https://www.cisa.gov/news-events/alerts/2024/10/02/cisa-adds-one-known-exploited-vulnerability-catalog
2. https://www.cisa.gov/news-events/alerts/2024/10/03/cisa-adds-one-known-exploited-vulnerability-catalog
3. https://www.cisa.gov/news-events/alerts/2024/10/08/cisa-adds-three-known-exploited-vulnerabilities-catalog
4. https://www.cisa.gov/news-events/alerts/2024/10/09/cisa-adds-three-known-exploited-vulnerabilities-catalog
5. https://www.cisa.gov/news-events/alerts/2024/10/15/cisa-adds-three-known-exploited-vulnerabilities-catalog
6. https://www.cisa.gov/news-events/alerts/2024/10/17/cisa-adds-one-known-exploited-vulnerability-catalog
7. https://www.trendmicro.com/en_us/research/24/j/earth-simnavaz-cyberattacks.html
8. https://infosec.exchange/@SophosXOps/113284564225476186
9. https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575
10. https://notes.netbytesec.com/2024/10/lemonduck-unleashes-cryptomining.html
11. https://securityonline.info/psaux-ransomware-is-exploiting-two-max-severity-flaws-cve-2024-51567-cve-2024-51568-in-cyberpanel/
12. https://www.securityweek.com/recent-version-of-lightspy-ios-malware-packs-destructive-capabilities/