loginsoft

Monthly Report

Threat & Vulnerabilities Report – November 2024

Executive Summary

November saw a significant expansion in CISA's Known Exploited Vulnerabilities (KEV) catalog, with 22 critical flaws spanning multiple high-profile vendors. Palo Alto Networks accounted for five vulnerabilities, while Microsoft, Apple, PTZ Optics, and VMware vCenter Server each contributed two high-impact vulnerabilities, showcasing a broad spectrum of attack surfaces being targeted.

In a series of critical cybersecurity findings, Google addressed an actively exploited zero-day vulnerability in the Android Framework. Kaspersky identified a new campaign using the "bring your own vulnerable driver" (BYOVD) technique to deploy SteelFox malware, which achieves SYSTEM-level access on Windows systems for cryptocurrency mining and data theft. CloudSEK reported increased activity from the AndroxGh0st botnet, exploiting vulnerabilities and possibly collaborating with the Mozi botnet to enhance its reach.

Meanwhile, Fortinet flagged a phishing campaign delivering a fileless version of Remcos RAT via malicious Excel files, and ClearSky revealed the ongoing exploitation of a Microsoft Windows vulnerability since July 2024 to deploy SparkRAT malware. Furthermore, the Helldown ransomware group has been exploiting vulnerabilities in Zyxel firewalls to gain initial access to targeted networks.

Actively Exploited Vulnerabilities

CVE-ID	Affected Product	Severity	Description	Zero-day	Actively Exploited	Abused by malware	CISA KEV	OSS
CVE-2024-8956			An authentication bypass vulnerability could allow attackers to gain unauthorized access to the camera's administrative interface without needing valid credentials, effectively	No	Yes	No	Yes	False

	PTZOptics PT30X-SDI/NDI Cameras	Critical	bypassing security controls.					
CVE-2024-8957			A command injection vulnerability may allow attackers to execute arbitrary commands, potentially granting them full control over the affected system.	No	Yes	No	Yes	False
CVE-2024-43093	Android Framework Component	Critical	An elevation of privilege vulnerability could enable attackers to gain unauthorized access and perform actions with higher-level privileges than intended.	Yes	Yes	No	Yes	True
CVE-2024-5910	Palo Alto Networks Expedition	Critical	A critical authentication flaw could enable attackers with network access to compromise an administrator account, granting them full control over the system.	No	Yes	No	Yes	False
CVE-2024-4577	PHP	Critical	A critical argument injection vulnerability that can be leveraged to achieve remote code execution.	No	Yes	Yes	Yes	False
CVE-2024-36401	OSGeo GeoServer GeoTools	Critical	An eval injection vulnerability that could result in remote code execution	No	Yes	Yes	Yes	True

CVE-2024-49039	Microsoft Windows	High	An Elevation of Privilege vulnerability in the Windows task scheduler	Yes	Yes	No	Yes	False
CVE-2024-43451	Microsoft Windows	Medium	Windows NTLM hash disclosure spoofing vulnerability.	Yes	Yes	Yes	Yes	False
CVE-2024-10914	D-Link NAS	Critical	A command injection vulnerability that allows unauthenticated attackers to inject arbitrary shell commands via specially crafted HTTP GET requests.	No	Yes	No	No	False
CVE-2024-9463	Palo Alto Networks Expedition	Critical	An unauthenticated OS command injection vulnerability in the Palo Alto Networks Expedition	No	Yes	No	Yes	False
CVE-2024-9465	Palo Alto Networks Expedition	Critical	An unauthenticated SQL injection vulnerability in the Palo Alto Expedition	No	Yes	No	Yes	False
CVE-2024-0012	Palo Alto Networks PAN-OS software	Critical	An authentication bypass vulnerability in PAN-OS allows unauthenticated attackers with network access to the management web interface to escalate privileges to	No	Yes	Yes	Yes	False

			administrator level.					
CVE-2024-9474	Palo Alto Networks PAN-OS software	Medium	An OS command injection vulnerability allows administrators with access to the management web interface to escalate their privileges and execute actions on the firewall with root-level permissions	No	Yes	No	Yes	False
CVE-2024-11120	GeoVision Devices	Critical	A pre-authentication command injection vulnerability in the GeoVision	Yes	Yes	Yes	No	False
CVE-2024-11680	ProjectSend	Critical	An improper authentication vulnerability allows remote, unauthenticated attackers to exploit the issue by sending specially crafted HTTP requests to the application's configuration	No	Yes	No	No	False
CVE-2024-11667	Zyxel firewall	High	A directory traversal vulnerability identified in the web management interface of Zyxel ZLD firewall firmware	No	Yes	Yes	No	False
CVE-2024-1212	Progress Kemp LoadMaster	Critical	A command injection vulnerability in the Kemp	No	Yes	No	Yes	False

			LoadMaster allows unauthenticated attackers to gain access to the LoadMaster management interface, potentially compromising the system's integrity and security.					
CVE-2024-8068	Citrix Session Recording	Medium	Privilege escalation to NetworkService Account access in Citrix Session Recording	Yes	Yes	No	No	False
CVE-2024-8069	Citrix Session Recording	Medium	Limited remote code execution with privilege of a NetworkService Account access	Yes	Yes	No	No	False
CVE-2024-38812	VMware vCenter Server	Critical	A heap overflow vulnerability allows a malicious actor with network access to send specially crafted packets, potentially resulting in remote code execution.	No	Yes	No	Yes	False
CVE-2024-38813	VMware vCenter Server	Critical	A privilege escalation vulnerability allows an attacker with network access to gain root privileges by sending a specially crafted network packet.	No	Yes	No	Yes	False

CVE-2024-44308	Apple	High	A vulnerability in JavaScriptCore could allow arbitrary code execution when processing maliciously crafted web content.	Yes	Yes	No	Yes	False
CVE-2024-44309	Apple	Medium	A cookie management vulnerability in WebKit could enable cross-site scripting (XSS) attacks when handling specially crafted malicious web content, potentially compromising user data and security.	Yes	Yes	No	Yes	False
CVE-2024-21287	Oracle Agile PLM Framework	High	An incorrect authorization vulnerability that could be exploited remotely without requiring any authentication.	No	Yes	No	Yes	False
CVE-2024-42057	Zyxel firewall series	High	A command injection vulnerability in the IPSec VPN feature of certain firewall versions enables unauthenticated attackers to execute arbitrary OS commands. This can be exploited by sending a specially crafted	No	Yes	Yes	No	False

			username to the vulnerable device, potentially compromising its integrity.					
CVE-2023-1389	TP-Link Archer AX21 (AX1800)	High	A command injection vulnerability exists in the country form of the **/cgi-bin/luci;stok=/locale** endpoint on the web management interface, potentially allowing attackers to execute unauthorized commands.	No	Yes	Yes	Yes	False
CVE-2023-28461	Array Networks AG and vxAG ArrayOS	Critical	An improper authentication vulnerability that could be exploited remotely, potentially allowing attackers to execute arbitrary code on the affected systems	No	Yes	Yes	Yes	False
CVE-2022-1040	Sophos Firewall	Critical	An authentication bypass vulnerability specifically in the User Portal and Webadmin components, that allows remote attackers to execute arbitrary code.	No	Yes	Yes	Yes	False

CVE-2022-21587	Oracle E-Business Suite	Critical	An unauthenticated remote code execution vulnerability in the Oracle EBusines Suite that allows unauthenticated attackers to remotely upload malicious files via HTTP, potentially leading to full control over the affected application.	No	Yes	Yes	Yes	False
CVE-2021-41773	Apache HTTP	High	A path traversal vulnerability that allows an attacker with network access to use a crafted URL path to map and access files outside of the server's document root, effectively bypassing security controls.	No	Yes	Yes	Yes	False
CVE-2021-26086	Atlassian's Confluence Server and Data Center	Medium	A remote code execution vulnerability in the Questions for Confluence app within the Atlassian's Confluence Server and Data Center products where improper permissions handling could allow an unauthenticated	No	Yes	Yes	Yes	False

			attacker to execute arbitrary code on the server.					
CVE-2021-41277	Metabase	Critical	A vulnerability in Metabase, an open-source business intelligence tool, allows attackers to exploit a Local File Inclusion (LFI) issue within its custom GeoJSON map functionality.	No	Yes	Yes	Yes	False
CVE-2021-41285	Ballistix MOD Utility	High	A local privilege escalation vulnerability in the **MODAPI.sys** driver allows low-privileged users to leverage the **MmMapIoSpace** function to access physical memory, potentially leading to unauthorized access and system compromise.	No	Yes	Yes	No	False
CVE-2020-1472	Microsoft Windows Server versions with Active Directory	Critical	This vulnerability, also known as "Zerologon," is a critical security vulnerability that affects Windows Server operating systems and was disclosed by Microsoft in August 2020.	No	Yes	Yes	Yes	True
CVE-2020-14979	EVGA's Precision	High	A local privilege escalation vulnerability in	No	Yes	Yes	No	False

	X1 performanc e software		the WinRing0_1_2_0 driver service allows low-privileged users or attackers to execute arbitrary commands with SYSTEM-level privileges, posing a significant risk to system integrity and security.					
CVE-2019-16278	Nostromo nhttpd	Critical	A directory traversal vulnerability allows attackers to access directories outside the intended scope, potentially leading to unauthorized command execution and posing a significant risk for remote code execution.	No	Yes	No	Yes	False
CVE-2018-15133	Laravel Framework	High	A vulnerability that enables remote attackers to execute arbitrary code on affected systems by exploiting an unserialization flaw within the framework's encryption mechanism.	No	Yes	Yes	Yes	True
CVE-2018-10561	DASAN GPON	Critical	Authentication bypass vulnerability in	No	Yes	Yes	Yes	False

	home routers		the DASAN GPON home routers.					
CVE-2018-10562	DASAN GPON home routers	Critical	Command injection vulnerability in the DASAN GPON home routers.	No	Yes	Yes	Yes	False
CVE-2017-9841	PHPUnit	Critical	A vulnerability in the PHPUnit which is caused due to improper input validation within the framework's PHPUnit\Util\PHP file, which can allow an attacker to achieve remote code execution on the affected system.	No	Yes	Yes	Yes	True
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	False
CVE-2014-2120	Cisco Adaptive Security Appliance (ASA)	Medium	A cross-site scripting (XSS) vulnerability in the WebVPN login page of Cisco Adaptive Security Appliance (ASA) software that allows remote attackers to inject arbitrary webscript or HTML code via an unspecified parameter.	No	Yes	Yes	Yes	False

Ransomware Insights for November

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 November 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	88	• Education • Construction • Government	CVE-2020-1472
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,	69	• Education • Manufacture • Finance	• CVE-2020-1472

	especially within pivotal domains like Services and Goods, Manufacturing, Education, and Finance.			• CVE-2020-3259
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.	42	• Healthcare • Financial • Government Agencies • Manufacturing • Industrial Sectors • Telecommunications	Unknown
Inc Ransom	The Inc Ransom group is a sophisticated ransomware operation targeting large-scale organizations and enterprises. Known for its diverse attack methods, the group employs a combination of vulnerability exploitation, spear-phishing campaigns, and tailored ransomware deployment to compromise victims. Once inside a network, Inc Ransom uses advanced techniques to encrypt files, including partial encryption to optimize speed, targeting only key portions of large files.	22	• Education • Healthcare • Government Sectors	CVE-2023-3519
Play	The Play ransomware group, also identified as Balloonfly	21		

	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.		• 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	21	• Healthcare • Education • Research	Unknown

	activities associated with the recently dismantled Hive cartel.			
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 adaptive approach underscores Fog ransomware's escalating threat, as it increasingly prioritizes industries where operational disruption could drive substantial ransom demands.	20	• Education • Recreation	• CVE-2024-40711 • CVE-2024-40766
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.	18	• 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	15		

	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.		• Education • Healthcare	• CVE-2023-40044 • CVE-2023-4966 • CVE-2023-20269 • CVE-2023-27350 • CVE-2023-27351 • CVE-2022-36537 • CVE-2022-41082
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.	14	• Healthcare • Finance • Education • Government • Manufacturing	Unknown
Blacksuit	BlackSuit ransomware, a rebranded version of the	14		

	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.		• 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 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	13	• 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

	attackers. Initially adopting a double-extortion model, the group shifted its strategy towards data exfiltration attacks after releasing a free decryptor.			
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	10	• Healthcare • Finance • Insurance	Unknown

	provided by the attackers upon ransom payment. Additionally, RA World has shown a particular focus on healthcare organizations in the Latin American region, indicating a geographic as well as sector-based specificity in its targeting strategy.			
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

Conclusion

In conclusion, the cybersecurity landscape this month reveals an alarming increase in the frequency and sophistication of attacks. From the exploitation of zero-day vulnerabilities in critical systems to targeted ransomware campaigns leveraging weaknesses in enterprise products, attackers continue to develop increasingly sophisticated methods to infiltrate networks. The use of advanced techniques like BYOVD, phishing for fileless malware, and botnet integrations illustrates a shift toward more complex and harder-to-detect attack strategies. These trends underscore the urgency for organizations to prioritize comprehensive vulnerability management, improve threat detection capabilities, and adopt a proactive defense posture to mitigate the risk of emerging cyber threats.

Sources Cited:

1. https://www.cisa.gov/news-events/alerts/2024/11/04/cisa-adds-two-known-exploited-vulnerabilities-catalog
2. https://www.cisa.gov/news-events/alerts/2024/11/07/cisa-adds-four-known-exploited-vulnerabilities-catalog

3. https://www.cisa.gov/news-events/alerts/2024/11/14/cisa-adds-two-known-exploited-vulnerabilities-catalog
4. https://www.cisa.gov/news-events/alerts/2024/11/18/cisa-adds-three-known-exploited-vulnerabilities-catalog
5. https://www.cisa.gov/news-events/alerts/2024/11/21/cisa-adds-three-known-exploited-vulnerabilities-catalog
6. https://www.cisa.gov/news-events/alerts/2024/11/20/cisa-adds-two-known-exploited-vulnerabilities-catalog
7. https://www.cloudsek.com/blog/mozi-resurfaces-as-androxgh0st-botnet-unraveling-the-latest-exploitation-wave
8. https://securelist.com/steelfox-trojan-drops-stealer-and-miner/114414/
9. https://www.clearskysec.com/0d-vulnerability-exploited-in-the_wild/
10. https://www.fortinet.com/blog/threat-research/new-campaign-uses-remcos-rat-to-exploit-victims
11. https://labs.watchtowr.com/visionaries-at-citrix-have-democratised-remote-network-access-citrix-virtual-apps-and-desktops-cve-unknown/