loginsoft

Monthly Report

Threat & Vulnerabilities Report – December 2024

Executive Summary

This month, 16 new vulnerabilities were added to the CISA KEV catalog, emphasizing active threats across various technologies. Notable entries include two vulnerabilities each from Microsoft products, Reolink devices, NUUO NVRmini devices, and Cleo multiple products, showcasing the growing focus of attackers on both enterprise solutions and consumer-grade devices.

The Cl0p ransomware group has taken responsibility for attacks on Cleo products, showcasing their ongoing disruptive operations. Meanwhile, Mauri ransomware exploits vulnerabilities in Apache ActiveMQ servers to infiltrate systems. In another alarming development, Northwave identified the LITTLELAMB.WOOLTEA backdoor malware during a targeted attack on a Palo Alto Networks firewall, reflecting the increasing sophistication of cyber threats. Additionally, Kaspersky revealed that the Cloud Atlas group is leveraging advanced phishing campaigns to exploit Microsoft Office vulnerabilities, highlighting the persistent threat of cyber espionage against critical systems and popular platforms.

Actively Exploited Vulnerabilities

CVE-ID	Affected Product	Severity	Description	Zero-day	Actively Exploited	Abused by malware	CISA KEV	OSS
CVE-2024-12856	Four-Faith routers	High	An unauthenticated operating system command injection vulnerability in the Four-Faith industrial routers that allows attackers to execute arbitrary commands on vulnerable devices remotely.	Yes	Yes	No	No	False
CVE-2024-12356	BeyondTrust	Critical	A command injection vulnerability in BeyondTrust's Privileged Remote Access (PRA) and Remote Support (RS) products could enable an unauthenticated attacker to inject	No	Yes	No	Yes	False

			malicious commands.					
CVE-2024-55956	Cleo Harmony, VLTrader, and LexiCom	Critical	An unrestricted file upload vulnerability allows an unauthenticated attacker to import and execute arbitrary Bash or PowerShell commands on the host system by exploiting the default settings of the Autorun directory.	Yes	Yes	Yes	Yes	False
CVE-2024-50623	Cleo Harmony, VLTrader, and LexiCom	Critical	An unrestricted file upload and download vulnerability that can be exploited to achieve remote code execution with elevated privileges.	Yes	Yes	Yes	Yes	False
CVE-2024-35250	Microsoft Windows	High	A vulnerability in the Microsoft Windows Kernel-mode Driver involving an untrusted pointer dereference could allow attackers to execute malicious code with elevated system privileges upon successful exploitation.	No	Yes	No	Yes	False
CVE-2024-49035	Microsoft Partner Center	High	An improper access control vulnerability in the **partner.microsoft[.]complatform** enables an unauthenticated attacker to perform privilege escalation over a network, potentially compromising sensitive operations and data.	No	Yes	No	No	False
CVE-2024-20767	Adobe ColdFusion	High	An improper access control vulnerability in Adobe ColdFusion	No	Yes	No	Yes	False

			allows attackers to access or modify restricted files, potentially compromising sensitive information.					
CVE-2024-49138	Microsoft Windows	High	An Elevation of Privilege vulnerability in the Windows Common Log File System (CLFS) Driver	Yes	Yes	No	Yes	False
CVE-2024-51378	CyberPanel	Critical	An incorrect default permissions vulnerability enables authentication bypass and allows the execution of arbitrary commands by exploiting shell metacharacters in the **statusfile** property.	Yes	Yes	Yes	Yes	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	Yes	False
CVE-2024-11667	Zyxel Multiple Firewalls	Critical	A directory traversal vulnerability identified in the web management interface of Zyxel ZLD firewall firmware.	No	Yes	Yes	Yes	False
CVE-2024-45841	I-O DATA routers UD-LT1 and UD-LT1/EX	Medium	An attacker with access to a guest account could exploit this vulnerability to capture and potentially steal user credentials.	No	Yes	No	No	False
CVE-2024-47133	I-O DATA routers UD-LT1	High	This vulnerability enables an authenticated administrator to	No	Yes	No	No	False

	and UD-LT1/EX		execute arbitrary operating system commands, potentially allowing attackers to gain complete control over the device.					
CVE-2024-52564	I-O DATA routers UD-LT1 and UD-LT1/EX	High	A remote attacker could exploit this vulnerability to disable the firewall functionality of affected devices.	No	Yes	No	No	False
CVE-2024-11972	Hunk Companion	Critical	A vulnerability allowing the arbitrary installation of plugins via unauthenticated POST requests.	No	Yes	No	No	False
CVE-2024-53677	Apache Struts	Critical	A remote code execution vulnerability has been identified, allowing attackers to execute arbitrary code by exploiting weaknesses in the file upload mechanism.	No	Yes	No	No	False
CVE-2024-41713	Mitel MiCollab	Medium	A path traversal vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab that arises due to insufficient input validation.	No	Yes	No	No	False
CVE-2024-35286	Mitel MiCollab	Critical	A pre-authentication SQL injection vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab allows attackers to execute unauthorized database operations, potentially compromising sensitive information.	Yes	Yes	No	No	False

CVE-2024-3393	Palo Alto Networks PAN-OS	High	A denial-of-service (DoS) vulnerability has been identified in the DNS Security feature of Palo Alto Networks' PAN-OS software.	No	Yes	Yes	No	False
CVE-2024-33112	D-Link DIR-845L	High	A command injection vulnerability has been identified in D-Link DIR routers through the **hnap_main()** function.	Yes	Yes	No	Yes	False
CVE-2023-46604	Apache ActiveMQ and ActiveMQ Artemis	Critical	A remote execution vulnerability in the Apache ActiveMQ server, that can allow an attacker to execute malicious commands remotely and take complete control over the target system.	No	Yes	Yes	Yes	True
CVE-2023-45727	North Grid Proself	High	This vulnerability enables remote, unauthenticated attackers to execute XML External Entity (XXE) attacks. By sending a specially crafted XML request, the attacker can access and potentially read sensitive files stored on the server, including private account information	No	Yes	Yes	Yes	False
CVE-2022-23227	NUUO NVRmini 2 Devices	Critical	A missing authentication vulnerability in the NUUO NVRmini 2 devices.	No	Yes	No	Yes	False
CVE-2021-40407	Reolink RLC-410W IP Camera	Critical	An OS command injection vulnerability in the ReoLink IP camera.	No	Yes	No	Yes	False
CVE-2021-44207	Acclaim Systems	High	Use of Hard-Coded credentials	No	Yes	Yes	Yes	False

			vulnerability in the Acclaim Systems USAHERDS that could result in an arbitrary code execution on the susceptible servers					
CVE-2019-11001	Reolink Multiple IP Cameras	High	An OS command injection vulnerability in Reolink Multiple IP cameras.	No	Yes	No	Yes	False
CVE-2018-14933	NUUO NVRmini Devices	Critical	An OS command injection vulnerability in the NUUO NVRmini Devices.	No	Yes	No	Yes	False

Ransomware Insights for December

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 December Month	Targeted Industries	Vulnerabilities Abused Most
Clop	Clop ransomware is a sophisticated cyber threat first identified in 2019, known for its double-extortion tactics and targeted attacks on large organizations. Operated by the financially motivated cybercrime group TA505, Clop not only encrypts victim data but also exfiltrates sensitive information, threatening public disclosure unless a ransom is paid. The ransomware has been linked to high-profile attacks exploiting vulnerabilities in widely used software, including the MOVEit Transfer and Accellion File Transfer Appliance (FTA). Clop operators gain initial access through phishing campaigns, exploiting zero-day vulnerabilities,	68	• Healthcare • Bank • Education • Gaming • Transportation	• CVE-2024-55956 • CVE-2023-34362 • CVE-2023-47246 • CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351

	or leveraging compromised credentials.			
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.	52	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259
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	44	• Education • Construction • Government	CVE-2020-1472
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	22	• Healthcare	• CVE-2022-41080

	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.		• Media • Technology • Telecommunication	• CVE-2022-41040 • CVE-2022-41082 • CVE-2021-34523 • CVE-2020-12812 • CVE-2018-13379
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.	22	• Education • Recreation	• CVE-2024-40711 • CVE-2024-40766
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	14	• Healthcare • Education • Research	Unknown

	with the recently dismantled Hive cartel.			
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 Latin American region, indicating a geographic as well as sector-based specificity in its targeting strategy.	13	• Healthcare • Finance • Insurance	Unknown
Medusa	Emerging in 2019, the Medusa ransomware operates on a ransomware-as-a-service (RaaS)	13		

	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.		• Healthcare • Finance • Technology • Manufacturing	• CVE-2023-34362 • CVE-2023-47246 • CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2022-2295
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.	11	• Education • Healthcare	• 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.	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

	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.			
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.	8	• 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,	6	• Education • Healthcare • Government Sectors	CVE-2023-3519

	targeting only key portions of large files.			
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.	6	• Technology • Insurance • Manufacturing • Utilities • Real estate • Finance	• CVE-2021-42287 • CVE-2021-42278 • CVE-2021-34527 • CVE-2020-1472 • CVE-2019-16098

Conclusion

This month's cybersecurity landscape underscores the growing complexity and persistence of threats across various technologies. The inclusion of 16 new vulnerabilities in the CISA KEV catalog highlights significant risks to both enterprise systems and consumer-grade devices. Notable incidents, such as the Cl0p ransomware group's attacks on Cleo products and the discovery of the LITTLELAMB.WOOLTEA backdoor targeting Palo Alto Networks firewalls, illustrate the evolving tactics of cyber adversaries. These developments reaffirm the critical importance of proactive measures, timely patching, and robust defense strategies to address the ever-changing threat environment effectively.

External References:

- https://www.cisa.gov/news-events/alerts/2024/12/19/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2024/12/17/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2024/12/13/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2024/12/30/cisa-adds-one-known-exploited-vulnerability-catalog
- https://cybersecuritynews.com/malichus-malware-exploiting-cleo-0-day/
- https://www.cisa.gov/news-events/alerts/2024/12/16/cisa-adds-two-known-exploited-vulnerabilities-catalog

- https://www.cisa.gov/news-events/alerts/2024/12/10/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2024/12/04/cisa-adds-one-known-exploited-vulnerability-catalog
- https://securityonline.info/psaux-ransomware-is-exploiting-two-max-severity-flaws-cve-2024-51567-cve-2024-51568-in-cyberpanel/
- https://www.cisa.gov/news-events/alerts/2024/12/03/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2023/11/02/cisa-adds-one-known-exploited-vulnerability-catalog
- https://asec.ahnlab.com/en/85000/
- https://www.trendmicro.com/en_us/research/24/k/lodeinfo-campaign-of-earth-kasha.html
- https://www.cisa.gov/news-events/alerts/2024/12/18/cisa-adds-four-known-exploited-vulnerabilities-catalog

loginsoft

Connect with us

linkedin.com/loginsoft

x.com/loginsoft_inc

www.loginsoft.com