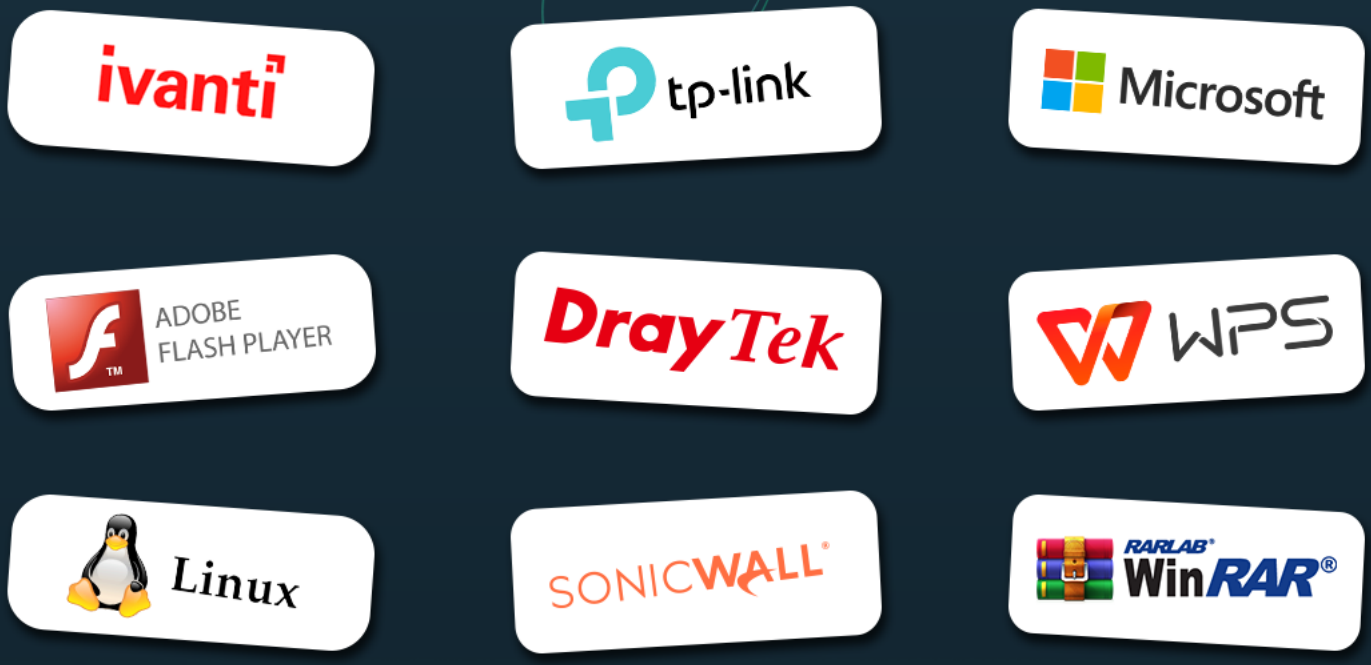
loginsoft

Monthly Report

Threat & Vulnerabilities Report - September 2024



Executive Summary

September saw a surge in critical vulnerabilities, with 26 CVEs added to the CISA Known Exploited Vulnerabilities (KEV) list, making it a month marked by significant cybersecurity risks.

Six Microsoft vulnerabilities, both historical and recently discovered have been added to the CISA KEV list, signaling a continued focus on securing Microsoft platforms. Meanwhile, Adobe Flash Player was back in the spotlight despite its 2020 end-of-life status as four of its vulnerabilities were recently added to the CISA KEV list, reminding that obsolete software can still pose serious risks. Additionally, Ivanti and DrayTek faced challenging times this month, with three vulnerabilities from each being added to the CISA KEV list, highlighting ongoing security concerns within their software and systems.

Ransomware activity escalated this month as Akira, Medusa, Mallox, and Conti targeted critical vulnerabilities, showcasing their relentless pursuit of victims. At the same time, Mirai botnet continued its aggressive campaign this month, actively targeting vulnerabilities in D-Link DIR and DrayTek Vigor routers, highlighting its relentless focus on exploiting network devices.

CVE-ID	Affected Product	Severity	Description	Zero-day	Actively Exploited	Abused by malware	CISA KEV	OSS
CVE-2024-43461	Microsoft Windows MSHTML platform	High	A spoofing vulnerability in the Windows MSHTML platform.	Yes	Yes	Yes	Yes	False
CVE-2024-38014	Windows Installer	High	An elevation of privilege vulnerability in the Windows Installer.	Yes	Yes	No	Yes	False
CVE-2024-38217	Windows Mark of the Web	Medium	A security feature bypass vulnerability in the Windows Mark-of-the-Web (MotW).	Yes	Yes	No	Yes	False
CVE-2024-38226	Microsoft Publisher	High	A security feature bypass vulnerability in the Microsoft Publisher	Yes	Yes	No	Yes	False

CVE-2024-43491	Microsoft Windows	Critical	A remote code execution vulnerability in the Microsoft Windows Update.	Yes	Yes	No	No	False
CVE-2024-6670	Progress Software's WhatsUp Gold	Critical	A SQL injection vulnerability in WhatsUp Gold allows attackers to bypass authentication and gain unauthorized access to encrypted user passwords.	No	Yes	No	Yes	False
CVE-2024-8190	Ivanti Cloud Services Appliance (CSA)	High	An OS command injection vulnerability in Ivanti Cloud Service Appliance that enables a remote authenticated attacker to achieve remote code execution.	No	Yes	No	Yes	False
CVE-2024-8963	Ivanti Cloud Services Appliance (CSA)	Critical	A path traversal vulnerability in Ivanti Cloud Service Appliance that can enable an attacker to bypass admin authentication and execute arbitrary commands on the appliance.	No	Yes	No	Yes	False
CVE-2024-7593	Ivanti's Virtual Traffic	Critical	Critical authentication bypass vulnerability in	No	Yes	No	Yes	False

	Manager (vTM)		Ivanti's Virtual Traffic Manager (vTM) that enables remote unauthenticated attackers to bypass authentication of the admin panel.					
CVE-2024-36401	OSGeo GeoServer GeoTools	Critical	An eval injection vulnerability in GeoServer that could result in remote code execution.	No	Yes	Yes	Yes	True
CVE-2024-45506	HAProxy products	High	A vulnerability in HAProxy can create an endless loop under certain conditions, leading to a system crash and a remote denial-of-service (DoS) attack.	No	Yes	No	No	False
CVE-2024-40766	SonicWall Firewall	Critical	An improper access control vulnerability in the SonicWall SonicOS management access and SSLVPN which could allow unauthorized access to resources and, under certain conditions, result in a firewall crash.	No	Yes	Yes	Yes	False
CVE-2024-7120	RAISECOM	Critical	A command injection vulnerability in	No	Yes	No	No	False

	Gateway devices		the RAISECOM Gateway devices enables remote attackers to execute malicious commands on the vulnerable systems.					
CVE-2024-47076	Common UNIX Printing System	High	The function **cfGetPrinterAttributes5** does not properly validate or sanitize the IPP attributes received from an IPP server, allowing attacker-controlled data to be passed through the rest of the CUPS system.	No	Yes	No	No	True
CVE-2024-47175	Common UNIX Printing System	High	The **ppdCreatePPDFromIPP2** function fails to validate or sanitize IPP attributes when writing them to a temporary PPD file, enabling the injection of attacker-controlled data into the resulting PPD file.	No	Yes	No	No	True
CVE-2024-47176	Common UNIX Printing System	High	Listens on **UDP INADDR_ANY:631**, accepting packets from any source, which can trigger	No	Yes	No	No	False

			a Get-Printer-Attributes IPP request directed to a URL controlled by an attacker.					
CVE-2024-47177	Common UNIX Printing System	Critical	The **foomatic-rip** utility allows arbitrary command execution through the **FoomaticRIPCommandLine** PPD parameter, potentially enabling exploitation by attackers.	No	Yes	No	No	False
CVE-2023-48788	Fortinet's EMS system	Critical	A SQL injection vulnerability in Fortinet's FortiClient EMS Software enables attackers to execute malicious code on vulnerable systems and gain initial access.	No	Yes	Yes	Yes	False
CVE-2023-38831	WinRAR	High	A vulnerability in WinRAR allows attackers to execute malicious code on a system by tricking users into opening a specially crafted archive file.	No	Yes	Yes	No	False
CVE-2023-25280	D-Link DIR-820 Router	Critical	An OS command injection vulnerability in the D-Link	No	Yes	Yes	Yes	False

			routers that can enable an attacker to elevate privileges to root via a crafted payload.					
CVE-2022-21445	Oracle JDeveloper	Critical	A remote code execution vulnerability in the Oracle JDeveloper application that enables attackers to execute arbitrary code on the vulnerable systems.	No	Yes	No	Yes	False
CVE-2021-20123	Draytek VigorConnect	High	An unauthenticated local file inclusion vulnerability DownloadFileServlet endpoint in that enables an unauthenticated attacker to download arbitrary files with root privileges	No	Yes	No	Yes	False
CVE-2021-20124	Draytek VigorConnect	High	An unauthenticated local file inclusion vulnerability WebServlet endpoint that enables an unauthenticated attacker to download arbitrary files	No	Yes	No	Yes	False

			with root privileges.					
CVE-2021-4043	GitHub repository GPAC	Medium	A null pointer dereference vulnerability in the GitHub repository GPAC that can be exploited to execute arbitrary code.	No	Yes	No	Yes	True
CVE-2020-0618	Microsoft SQL Server Reporting Services	High	A remote code execution vulnerability in the Microsoft SQL Server that can enable an attacker to execute arbitrary code in the context of Report Server service account.	No	Yes	Yes	Yes	False
CVE-2020-14644	Oracle WebLogic Server	Critical	A remote code execution vulnerability in the Oracle WebLogic Server that enables the attacker to gain complete control over the affected system.	No	Yes	No	Yes	False
CVE-2020-15415	DrayTek Vigor	Critical	An OS command injection vulnerability in the DrayTek Vigor router that enables unauthenticated attackers to execute malicious code on the vulnerable systems.	No	Yes	Yes	Yes	False

CVE-2019-1069	Microsoft Windows Task scheduler	High	An elevation of privilege vulnerability in the Windows task scheduler.	No	Yes	Yes	Yes	False
CVE-2019-0344	SAP Commerce Cloud	Critical	Deserialization of Untrusted Data Vulnerability AP Commerce Cloud allows attackers to execute malicious code on a target system by exploiting the unsafe deserialization process.	No	Yes	No	Yes	False
CVE-2017-1000253	Linux kernel	High	A stack-based buffer overflow vulnerability in the Linux Kernal that enables a local attacker to escalate privileges.	No	Yes	Yes	Yes	False
CVE-2016-3714	ImageMagicK	High	An improper input validation vulnerability in the ImageMagicK that enables an attacker to execute arbitrary code by crafting an image with malicious shell metacharacters.	No	Yes	No	Yes	True
CVE-2014-0497	Adobe Flash Player	High	An integral underflow vulnerability in the Adobe Flash Player that enables remote	No	Yes	Yes	Yes	False

			attackers to execute arbitrary code on the vulnerable systems.					
CVE-2014-0502	Adobe Flash Player	High	A double free vulnerability in Adobe Flash Player that enables remote attackers to execute arbitrary code on the vulnerable systems.	No	Yes	Yes	Yes	False
CVE-2013-0643	Adobe Flash Player	High	An incorrect default permissions vulnerability in the Adobe Flash player that enables a remote attacker to execute arbitrary code on the vulnerable systems.	No	Yes	No	Yes	False
CVE-2013-0648	Adobe Flash Player	High	A remote code execution vulnerability in the Adobe Flash player that can enable remote attackers to execute arbitrary code on vulnerable systems.	No	Yes	No	Yes	False

Ransomware Insights for September

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 September 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	55	• 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 media industries. It was observed that the group focused on	42	• Healthcare • Media • Technology • Telecommunication	• CVE-2021-34523 • CVE-2022-41080 • CVE-2022-41040 • CVE-2022-41082 • CVE-2018-13379 • CVE-2020-12812

	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.			
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.	22	• Healthcare • Finance • Technology • Manufacturing	• CVE-2022-2295 • CVE-2023-34362 • CVE-2023-47246 • CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351
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
cactus	Active since March 2023, Cactus ransomware has primarily focused	15	• commercial entities	• CVE-2023-41265 • CVE-2023-41266

	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.		• Lawfirms • Manufacturing	• CVE-2023-48365
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.	14	• Healthcare • Education • Research	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-	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

	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.			
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.	12	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259
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	• CVE-2023-40044 • CVE-2023-4966 • CVE-2023-20269 • CVE-2023-27350 • CVE-2023-27351 • CVE-2022-36537 • CVE-2022-41082
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	8	• Education • Healthcare • Manufacturing • Information Technology • Government sectors	CVE-2020-1472

	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.			
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.	8	• Education • Healthcare • Government sectors	CVE-2023-3519

Conclusion

September has emerged as a pivotal month in cybersecurity, with a record 26 CVEs added to the CISA KEV list, marking the highest number of additions in any month of 2024 to date. The ongoing exploitation of the vulnerabilities by ransomware groups such as Akira and Medusa emphasizes the need for vigilance and robust security measures. The Mirai botnet's relentless campaign showcases its continued focus on exploiting network infrastructure vulnerabilities underscoring the necessity for proactive security strategies. As we move forward, it is crucial for organizations to remain vigilant and prioritize security best practices to mitigate the risks posed by these and other emerging threats.

External References:

1. https://www.cisa.gov/news-events/alerts/2024/09/16/cisa-adds-two-known-exploited-vulnerabilities-catalog
2. https://www.cisa.gov/news-events/alerts/2024/09/10/cisa-adds-four-known-exploited-vulnerabilities-catalog
3. https://www.cisa.gov/news-events/alerts/2024/09/13/cisa-adds-one-known-exploited-vulnerability-catalog
4. https://www.cisa.gov/news-events/alerts/2024/09/19/cisa-adds-one-known-exploited-vulnerability-catalog
5. https://www.cisa.gov/news-events/alerts/2024/09/09/cisa-adds-three-known-exploited-vulnerabilities-catalog
6. https://www.cisa.gov/news-events/alerts/2024/09/17/cisa-adds-four-known-exploited-vulnerabilities-catalog
7. https://www.cisa.gov/news-events/alerts/2024/09/30/cisa-adds-four-known-exploited-vulnerabilities-catalog
8. Medusa Ransomware: A Growing Threat with a Bold Online Presence (bitdefender.com)
9. https://www.fortinet.com/blog/threat-research/threat-actors-exploit-geoserver-vulnerability-cve-2024-36401
10. https://www.theregister.com/2024/09/17/microsoft_zero_day_spoofing_flaw/
11. https://securelist.com/head-mare-hacktivists/113555/
12. https://www.tenable.com/blog/contileaks-chats-reveal-over-30-vulnerabilities-used-by-conti-ransomware-affiliates
13. https://www.darkreading.com/cyberattacks-data-breaches/mallox-ransomware-group-shifts-into-high-gear
14. https://thehackernews.com/2024/09/critical-linux-cups-printing-system.html