Monthly Report

loginsoft

Threat & Vulnerabilities Report - May 2024

Executive Summary

In May, seven zero-day vulnerabilities were discovered—four targeting Google Chrome and two affecting Microsoft Windows. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) added twelve vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog. Out of these, five are being actively exploited, granting threat actors administrative access for malicious activities. Notably, five of the identified vulnerabilities involve code injection flaws, which enable remote attackers to execute unauthorized commands on the compromised systems.

Below table listed May month Actively exploited and critical vulnerabilities

CVE-ID	Affected Product	Severity	Description	Zero-day	Actively Exploited	Abused by Malware/Threat actor	CISA KEV	OSS
CVE-2024-4671	Google Chrome	Critical	A use after free in visuals vulnerability in Google Chrome which when successfully exploited can permit an attacker to install programs, view, change or delete data and create new user accounts with administrative privileges.	Yes	Yes	Yes	Yes	True
CVE-2024-4761	Google Chrome	High	An out-of-bounds write issue in Google Chrome's V8 JavaScript Engine which can be leveraged by the attacker to execute arbitrary code and crash the application.	Yes	Yes	No	Yes	True
CVE-2024-4947	Google Chrome	High	A Type confusion bug in the V8 JavaScript engine that could allow an attacker to perform remote code execution attacks	Yes	Yes	No	Yes	True
CVE-2024-5274	Google Chrome	High	A type confusion vulnerability in the Google Chrome's V8 JavaScript and WebAssembly engine that can result in unexpected crashes and even remote code execution.	Yes	Yes	Yes	Yes	True
CVE-2024-30051	Microsoft Windows DWM core library	High	An Elevation of Privilege (EoP) vulnerability in the DWM core Library in Microsoft Windows that can be exploited by a local attacker to gain SYSTEM privileges.	Yes	Yes	Yes	Yes	False

CVE-2024-30040	Microsoft Windows DWM core library	High	A security feature bypass vulnerability in the MSHTML (Trident) Engine in Microsoft Windows that could be exploited by the attacker by using social engineering tactics via email, social media to convince a target user to open a specially crafted malicious document and then execute an arbitrary code.	Yes	Yes	No	Yes	False
CVE-2024-4978	JAVS Viewer	High	A software supply chain attack in JAVS Viewer, a component of the JAVA Suite 8 that allows users to produce, manage, publish, and view digital recordings of legal proceedings, business meetings	No	Yes	Yes	No	False
CVE-2024-24919	CheckPoin	High	An information disclosure vulnerability in multiple products of CheckPoint that can enable the attackers to read certain data from Internet- connected gateways that with remote access VPN or mobile access enabled.	Yes	Yes	Yes	Yes	
CVE-2024-1086	Linux Kernel	High	A use-after-free vulnerability in the Linux Kernel's netfilter: nf_tables component that can be leveraged by the attackers to gain local privilege escalation.	No	Yes	Yes	No	
CVE-2024-2194	WordPress	High	A cross-site scripting vulnerability in the WP Statistics Plugin for WordPress that could potentially lead to arbitrary code execution.	No	Yes	No	No	
CVE-2023-6961	WordPress	High	A cross-site scripting vulnerability in the WP Meta SEO Plugin caused due to inadequate input sanitization and output escaping, that makes it possible for attackers to inject malicious scripts.	No	Yes	Yes		

CVE-2023-43208	Mirth Connect	Critical	A pre-authenticated remote code execution vulnerability in NextGen Mirth Connect that was exploited successfully against several health organizations by NodeZero, a pentesting tool of Horizon3.ai.	No	Yes	No	Yes	False
CVE-2023-7028	GitLab Community Edition and Gitlab Enterprise edition	High	An account-take-over vulnerability that could allow an attacker to take over the GitLab administrator account without requiring the user interaction.	No	Yes	No	Yes	False
CVE-2023-20198	Cisco IOS XE software	Critical	A privilege escalation vulnerability in the Web UI feature, that could allow an attacker to create an administrative user.	Yes	Yes	Yes	Yes	False
CVE-2023-40000	LiteSpeed Cache plugin for WordPress	High	A stored cross-site scripting (XSS) vulnerability in the LiteSpeed Cache plugin for WordPress that allows an unauthorized user to elevate privileges by using specially crafted HTTP requests.	No	Yes	Yes	No	False
CVE-2023-26801	LB-LINK	Critical	A command injection vulnerability in LB-LINK products which when successfully exploited could allow a remote attacker to execute arbitrary commands on the affected systems.	No	Yes	Yes	No	False
CVE-2021-40655	D-Link	High	An information disclosure vulnerability in the D-Link-DIR-605 B2 Firmware Version: 2.01 MT that can be leveraged by the attacker to retrieve login credentials by forging a post request to the / getcfg.php page.	No	Yes	No	Yes	False
CVE-2020-17519	Apache Flink	High	A directory traversal vulnerability in the REST API of Apache Flink that enables an attacker to potentially read any file on the local filesystem of the JobManager.	No	Yes	No	Yes	False
CVE-2018-4233	Web browser engine in Apple	High	A code execution vulnerability affecting WebKit - web browser engine	No	Yes	Yes	No	

			that can enable remote attackers to execute arbitrary commands on the targeted device.					
CVE-2018-4404	Apple operating systems	High	A memory corruption vulnerability affecting Apple's iOS and macOS operating systems could potentially allow an attacker with network access to take complete control over a compromised device	No	Yes	Yes	No	
CVE-2017-3506	Oracle Fusion Middleware	High	An operating system command injection vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware that allows an unauthenticated attacker via HTTP network access to compromise the Oracle WebLogic Server.	No	Yes	Yes	Yes	
CVE-2015-2051	D-Link DIR-645 routers	High	A remote code execution vulnerability that permits the attackers to execute malicious commands via a GetDeviceSettings action on the HNAP interface of targeted devices remotely.	No	Yes	Yes	Yes	False
CVE-2014-100005	D-Link	Medium	A Cross-Site Request Forgery (CSRF) vulnerability present in the D-Link DIR600 Router that allows the attacker to perform malicious actions on behalf of an authenticated user which results in creation of fraud administrator accounts and exposure of sensitive user credentials	No	Yes	No	Yes	False
CVE-2008-0166	Debain based operating systems like Debain and Ubuntu	High	A vulnerability in the OpenSSL library used by Debian-based operating systems, including Debain and Ubuntu. This vulnerability arises due to a predictable random number generator which makes it easier for the remote attackers to carry out brute force attacks against cryptographic keys.	No	No	No	No	True

Ransomware Insights for May

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 May	Targeted Industries	Vulnerabilities Abused Most
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.	114	• 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
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	57	• 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	31	• Healthcare • Media • Technology • Telecommunication	• CVE-2021-34523 • CVE-2022-41080 • CVE-2022-41040 • CVE-2022-41082 • CVE-2018-13379 • CVE-2020-12812

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

8Base	Despite a significant surge in activity during the summer of 2023, the 8Base ransomware group has largely operated in obscurity. Employing a combination of encryption and "name-and-shame" tactics, the group coerces victims into paying ransoms. Notably, 8Base follows an opportunistic compromise pattern, targeting victims across diverse industries. Despite the extensive compromises, details about the identities, methodology, and motivations behind the group's actions remain elusive. Examination of their ransomware samples indicates the use of a customized Phobos with SmokeLoader.	18	• Business service • Finance • Manufacture • Information technology	• CVE-2023-35078 • CVE-2023-3519
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.	18	• Education • Healthcare	• CVE-2023-40044 • CVE-2023-4966 • CVE-2023-20269 • CVE-2023-27350 • CVE-2023-27351 • CVE-2022-36537 • CVE-2022-41082
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.	18	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259
BlackBasta	Black Basta is a ransomware group operating as ransomware-as-a-	17	• Technology • Insurance	• CVE-2019-16098 • CVE-2021-42278

	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.		• Manufacturing • Utilities • Real estate • Finance	• CVE-2020-1472 • CVE-2021-34527 • CVE-2019-16098 • CVE-2021-42287
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 attackers. Initially adopting a double-extortion model, the group shifted its strategy towards data exfiltration attacks after releasing a free decryptor.	14	• 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

Conclusion

This report highlights the vulnerabilities actively exploited in May 2024. During this period, threat actors leveraged these weaknesses to deploy malware such as QakBot, GateDoor/RustDoor, and Mirai. To address these threats effectively, continuous system monitoring is essential. Additionally, regularly updating software to the latest versions, implementing robust security measures, and enforcing least privilege access controls are critical strategies for mitigating risks.

Sources Cited:

1. https://www.stormshield.com/news/security-alert-cve-2023-7028-stormshield-products-response/
2. https://www.rapid7.com/blog/post/2023/10/17/etr-cve-2023-20198-active-exploitation-of-cisco-ios-xe-zero-day-vulnerability/
3. https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_9.html

4. https://www.techradar.com/pro/security/watch-out-hackers-can-exploit-this-plugin-to-gain-full-control-of-your-wordpress-site
5. https://msrc.microsoft.com/update-guide/releaseNote/2024-May
6. https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2024-058
7. https://www.cisa.gov/news-events/alerts/2024/05/16/cisa-adds-three-known-exploited-vulnerabilities-catalog
8. https://www.cisa.gov/news-events/alerts/2024/05/20/cisa-adds-two-known-exploited-vulnerabilities-catalog
9. https://www.fortiguard.com/threat-signal-report/5460/nextgen-healthcare-mirth-connect-rce-cve-2023-43208-cve-2023-37679
10. https://socprime.com/blog/cve-2023-43208-detection-nextgens-mirth-connect-rce-vulnerability-exposes-healthcare-data-to-risks/
11. https://unit42.paloaltonetworks.com/network-attack-trends-winter-2020/
12. https://medium.com/s2wblog/rustdoor-and-gatedoor-a-new-pair-of-weapons-disguised-as-legitimate-software-by-suspected-34c94e558b40
13. https://www.spiceworks.com/it-security/cyber-risk-management/news/chrome-security-alert-fourth-zero-day-exploit-patched/
14. https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_23.html
15. https://blog.checkpoint.com/security/enhance-your-vpn-security-posture
16. https://www.cisa.gov/news-events/alerts/2024/05/30/cisa-adds-two-known-exploited-vulnerabilities-catalog
17. https://www.fastly.com/blog/active-exploitation-unauthenticated-stored-xss-vulnerabilities-wordpress/
18. https://cybersecuritynews.com/check-point-vpn-zero-day-vulnerability/
19. https://16years.secvuln.info/
20. https://securityonline.info/d-link-router-and-modem-vulnerabilities-are-being-exploited-by-satori-iot-botnet/

loginsoft

Connect with us

linkedin.com/loginsoft

x.com/loginsoft

www.loginsoft.com