Monthly Report

loginsoft

# Threat & Vulnerabilities Report - June 2024

# Executive Summary

In June, three zero-day vulnerabilities were identified, affecting Mali GPU kernel Driver, Google Pixel firmware and Microsoft Windows Error reporting service.

The Cybersecurity and Infrastructure Security Agency added nine CVE's to its Known Exploited Vulnerabilities (KEV) catalog. Of these, three are actively exploited in the wild, allowing threat actors to perform malicious activities with administrative privileges. Additionally, two of these vulnerabilities were code injection flaws, allowing remote attackers to execute malicious commands on the affected systems whereas two of these were authentication bypass vulnerabilities.

Below table listed by June month actively exploited and critical vulnerabilities.

| CVE-ID | Affected Product | Severity | Description | Zero-day | Actively Exploited | Abused by Malware | CISA KEV | OSS |
|---|---|---|---|---|---|---|---|---|
| CVE-2024-4610 | • Bifrost GPU Kernel Driver<br>• Valhall GPU Kernel Driver | High | A vulnerability in Mali GPU kernel Driver that involves improper GPU memory processing operations that can be leveraged by a local non-privileged user to gain access to already free memory. | Yes | Yes | No | Yes | False |
| CVE-2024-4577 | PHP | Critical | A critical argument injection vulnerability in PHP that can be leveraged to achieve remote code execution. | No | Yes | Yes | Yes | False |
| CVE-2024-30080 | Microsoft Message Queuing (MSMQ) | Critical | A critical remote code execution vulnerability in Microsoft Message Queuing (MSMQ) that can be exploited by a remote attacker to execute malicious commands and gain complete control over the affected system. | No | No | No | No | False |
| CVE-2024-32896 | Google Pixel Firmware | Critical | A critical elevation of privilege vulnerability in the Pixel Firmware. | Yes | Yes | No | Yes | True |
| CVE-2024-4358 | Progress Telerik Report Server | Critical | Critical authentication bypass vulnerability in the Progress Telerik Report Server which when exploited successfully can enable an attacker to take complete control over the affected server. | No | Yes | No | Yes | False |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CVE-2024-26169 | Windows Error Reporting service | High | An elevation of privilege vulnerability in the Windows Error Reporting service that can be exploited to gain SYSTEM privileges. | Yes | Yes | Yes | Yes | False |
| CVE-2024-6045 | D-Link wireless routers | High | An undisclosed factory testing backdoor that could enable attackers within the local network to gain unauthorized access to the router's Telnet service by utilizing default administrator credentials. | No | No | No | No | False |
| CVE-2024-37902 | Deep Java Library (DJL) | Critical | A critical path traversal vulnerability in the Deep Java Library (DJL) which enables the attackers to rewrite important system files and take complete control of the affected systems | No | No | No | No | True |
| CVE-2024-28995 | SolarWinds Serv-U file transfer software | High | A directory traversal vulnerability in SolarWinds Serv-U file transfer software that enables unauthorized attackers to potentially read confidential files present in the server hosting the software. | No | Yes | No | No | False |
| CVE-2024-29973 | Zyxel NAS326 and NAS542 devices | Critical | A command injection vulnerability in the "**setCookie**" parameter that enables an unauthenticated attacker to execute OS commands via specially crafted HTTP POST request. | No | Yes | Yes | No | False |
| CVE-2024-5806 | Progress MOVEit file transfer software product | Critical | A critical authentication bypass vulnerability affecting the SSH File Transfer Protocol (SFTP) module in the Progress MOVEit file transfer software product. | No | Yes | No | No | False |
| CVE-2023-32191 | Rancher Kubernetes Engine | Critical | A critical vulnerability in the Rancher Kubernetes Engine poses a severe risk to the security and integrity of Kubernetes clusters. | No | No | No | No | True |
| CVE-2023-21839 | Oracle WebLogic Server | High | A remote code execution vulnerability in the Oracle WebLogic Server | No | Yes | Yes | Yes | False |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | which could potentially result in the attackers taking full control of the affected system. | | | | | |
| CVE-2023-20867 | VMware tools | Low | An authentication bypass vulnerability in VMware tools that allows a fully compromised ESXi host to fail to authenticate host-to-guest operations thereby impacting the confidentiality and integrity of the guest virtual machine. | Yes | Yes | Yes | Yes | True |
| CVE-2022-22948 | VCenter Server | Medium | An information disclosure vulnerability in the VMware vCenter that exposes sensitive information due to improper file permissions. | Yes | Yes | Yes | No | False |
| CVE-2022-41328 | Fortinet FortiOS | High | An improper path traversal vulnerability in the Fortinet FortiOS that can allow privileged attackers to read and write arbitrary files via crafted CLI commands. | Yes | Yes | Yes | Yes | False |
| CVE-2022-42475 | • Fortinet'<br>• FortiOS<br>• FortiPro | Critical | A critical heap-based buffer overflow vulnerability in the SSL VPN component of Fortinet's FortiOS and FortiProxy devices which when successfully exploited by a remote unauthenticated attacker can lead to arbitrary code execution on the affected devices. | No | Yes | Yes | Yes | False |
| CVE-2022-24816 | GeoSolutions JAI-EXT | Critical | A critical remote code execution vulnerability in the JAI-EXT which is an open-source project that aims to extend the Java Advanced Imaging (JAI) API which can be leveraged by an attacker via a malicious Jiffle script provided through a network request. | No | Yes | No | Yes | True |
| CVE-2022-2586 | Linux Kernel | High | A use-after-free vulnerability in the nftables (NFT) framework of the Linux Kernel which when successfully exploited can allow an attacker to execute arbitrary codes with root privileges. | No | Yes | Yes | Yes | True |
| CVE-2020-13965 | Roundcube Webmail | Medium | A storage Cross-site scripting (XSS) vulnerability in the Roundcube Webmail that leverages an attacker to | No | Yes | No | Yes | True |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | bypass the script filter and execute malicious JavaScript on the affected systems | | | | | |
| 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. It resides in the Netlogon Remote Protocol (MS-NRPC), which is used for authentication in Active Directory environments. Specifically, the vulnerability arises from an improper implementation of the cryptographic algorithm used in the Netlogon authentication process. | No | Yes | Yes | Yes | True |
| CVE-2019-9082 | Think PHP | High | A critical remote code execution vulnerability in the Open Source BMS which exists due to improper handling of the user input in the invokefunction function of the ThinkPHP framework. This can be exploited by the attacker via specially crafted HTTP request including a malicious code in it. | No | Yes | Yes | Yes | False |
| CVE-2018-20062 | Think PHP | Critical | A critical remote code execution vulnerability in NoneCms which exists due to improper verification on user-supplied input within the filter parameter of the ThinkPHP framework. This can be exploited by the attacker by crafting a malicious URL that injects a code when the program processes it. | No | Yes | Yes | Yes | False |

# Ransomware Insights for June

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 June | Targeted Industries | Vulnerabilities Abused Most |
|---|---|---|---|---|
| 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. | 41 | • Healthcare<br>• Media<br>• Technology<br>• Telecommunication | • CVE-2021-34523<br>• CVE-2022-41080<br>• CVE-2022-41040<br>• CVE-2022-41082<br>• CVE-2018-13379<br>• CVE-2020-12812 |
| 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 | 39 | • Education<br>• Construction<br>• Government | • CVE-2020-1472 |

| | | | | |
|---|---|---|---|---|
| | 10th to March 4th on its data leak site | | | |
| **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. | 31 | • Education<br>• Manufacture<br>• Finance | • CVE-2020-1472<br>• CVE-2020-3259 |
| **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. | 21 | • Healthcare<br>• Finance<br>• Technology<br>• Manufacturing | • CVE-2022-2295<br>• CVE-2023-34362<br>• CVE-2023-47246<br>• CVE-2023-0669<br>• CVE-2023-27350<br>• CVE-2023-27351 |
| **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. | 20 | • Education<br>• Healthcare<br>• Government sectors | • CVE-2023-3519 |
| **Blacksuit** | BlackSuit ransomware, a rebranded version of the infamous Royal ransomware, emerged in May 2023 following intensified law | 20 | • Information technology<br>• Government<br>• Retail | • Unknown |

| | | | | |
|---|---|---|---|---|
| | 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 | | • Manufacturing | |
| **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. | 19 | • Education<br>• Healthcare<br>• Technology<br>• Manufacture<br>• Utilities<br>• Construction<br>• Entertainment | • CVE-2023-40044<br>• CVE-2023-4966<br>• CVE-2023-20269<br>• CVE-2023-27350<br>• CVE-2023-27351<br>• CVE-2022-36537<br>• CVE-2022-41082<br>• CVE-2024-1708<br>• CVE-2024-1709 |
| **cactus** | Active since March 2023, Cactus ransomware has primarily focused 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. | 18 | • commercial entities<br>• Lawfirms<br>• Manufacturing | • CVE-2023-41265<br>• CVE-2023-41266<br>• CVE-2023-48365 |
| **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 | 16 | • Education<br>• Healthcare | • CVE-2023-40044<br>• CVE-2023-4966<br>• CVE-2023-20269<br>• CVE-2023-27350<br>• CVE-2023-27351<br>• CVE-2022-36537<br>• CVE-2022-41082 |

| | | | | |
|---|---|---|---|---|
| | sectors, particularly in nations such as Thailand and Indonesia. | | | |
| **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. | 15 | • Technology<br>• Insurance<br>• Manufacturing<br>• Utilities<br>• Real estate<br>• Finance | • CVE-2019-16098<br>• CVE-2021-42278<br>• CVE-2020-1472<br>• CVE-2021-34527<br>• CVE-2019-16098<br>• CVE-2021-42287 |
| **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. | 13 | • Healthcare<br>• Education<br>• 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-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 | 12 | • Healthcare<br>• Banking<br>• Utilities<br>• Insurance | • CVE-2023-27350<br>• CVE-2022-37042<br>• CVE-2022-27925<br>• CVE-2021-4034<br>• CVE-2021-34523<br>• CVE-2021-34473<br>• CVE-2021-31207 |

| | | | | |
|---|---|---|---|---|
| | attacks after releasing a free decryptor. | | | |
| **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. | 9 | • Business service<br>• Finance<br>• Manufacture<br>• Information technology | • CVE-2023-35078<br>• CVE-2023-3519 |
| **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 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. | 7 | • Education<br>• Healthcare<br>• Manufacturing<br>• Information Technology<br>• Government sectors | • CVE-2020-1472 |

# Conclusion

This monthly report highlights several vulnerabilities affecting various systems and software. During this month, threat actors leveraged these security flaws to deploy ransomwares such as **TellYouThePass**, **BlackBasta**, backdoors such as **REPTILE, MEDUSA** and botnets like **Mirai**. These vulnerabilities demonstrate the ever-evolving nature of the cyber threat landscape and the importance of continuous

vigilance in maintaining a strong security posture. Additionally, regularly updating the software to latest versions, implementing robust security measures and enforcing least privilege access controls are important strategies for mitigating risks.

## Sources Cited:


1. https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations
2. https://thehackernews.com/2024/06/chinese-cyber-espionage-group-exploits.html
3. https://www.fortinet.com/blog/psirt-blogs/fg-ir-22-369-psirt-analysis
4. https://securityonline.info/d-link-routers-exposed-critical-backdoor-vulnerability-discovered-cve-2024-6045/#google_vignette
5. https://securityonline.info/cve-2024-37902-cvss-10-critical-flaw-in-deep-java-library-opens-door-to-system-takeover/
6. https://www.cisa.gov/news-events/alerts/2024/06/13/cisa-adds-three-known-exploited-vulnerabilities-catalog
7. https://www.tenable.com/cve/CVE-2023-32191
8. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-30080
9. https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-linked-to-windows-zero-day-attacks/
10. https://www.zerodayinitiative.com/advisories/ZDI-24-561/
11. https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities
12. https://www.akamai.com/blog/security-research/2024-thinkphp-applications-exploit-1-days-dama-webshell
13. https://fortiguard.fortinet.com/threat-signal-report/5142
14. https://labs.watchtowr.com/no-way-php-strikes-again-cve-2024-4577/
15. https://threatprotect.qualys.com/2023/03/03/jai-ext-remote-code-execution-vulnerability-cve-2022-24816/
16. https://www.vicarius.io/vsociety/posts/use-after-free-vulnerability-linked-chain-between-nft-tables-cve-2022-2586
17. https://thehackernews.com/2024/06/excobalt-cyber-gang-targets-russian.html
18. https://www.securityweek.com/cisa-warns-of-exploited-geoserver-linux-kernel-and-roundcube-vulnerabilities/
19. https://cybersecuritynews.com/zyxel-nas-devices-under-attack/
20. https://www.theregister.com/2024/06/24/mirailike_botnet_zyxel_nas/