August 30, 2021

# INFOSEC WEEKLY

#MADE4SECURITY

- VMware issues security updates addressing flaws affecting multiple products
- Critical Cosmos Database Flaw Affected Thousands of Microsoft Azure Customers
- F5 Releases critical Security Patch for BIG-IP and Big-IQ Devices
- Flaws found in Opensource elFinder File Manager
- Kaseya Issues Patches for Two New 0-Day Flaws Affecting Unitrends Servers

CryptoGen Nepal

## Introduction to InfoSec Weekly

InfoSec Weekly is a compilation of security related news feed that aims to update the readers about cyber security, cyber threats, malware attacks, new technologies and cyber security awareness every week. We primarily cover events and news related to offensive side of the Information Security such as hacking, password and sensitive information leakage, new vulnerabilities and important CVE's that can impact an individual or an organization. We also aim to provide defensive tactics to overcome known vulnerabilities that can protect organizations and individuals from any attacks.

Our main aim is to spread awareness regarding various cyber related threats.

## About Us

We are a team of security enthusiasts with an aim to provide various Information Security Services to organizations. Our company aims to provide professional grade cyber security solutions for all your Information Technology infrastructures. Our team has been demonstrating penetration testing skills using methodologies such as OSSTMM, NIST and OWASP. We aim to help companies protect their valuable data from any internal or external threats. Our team members have been practicing their skills to detect and report vulnerabilities in a live environment. Organizations such as Google, Facebook, Twitter, Yahoo!, eBay, eset, BugCrowd, under armour, Coinbase, CCM, etc. have recognized our team members for reporting vulnerabilities and have helped these organizations from malicious users. Our team's professional work experience consists of various Government organizations, National and International based private organizations, INGOs, etc. Our Services ranges from VAPT, Incident Response, Information Security Training, Endpoint threat analysis, Cyber security consultant, etc.

| VMware issues security updates addressing flaws affecting multiple products | |
|---|---|
| **Description** | |
| VMware has issued patches to fix vulnerabilities in various products that could allow attackers to potentially take control of an affected system. Also, VMware has issued patches to fix a XSS vulnerability that affected VMware vRealize log insight and VMware Cloud Foundation following the improper user input validation that allowed perpetrators to inject malicious payloads through the log insight UI which executes after the victim accesses the shared dashboard link. | |
| Source | https://thehackernews.com/2021/08/vmware-issues-patches-to-fix-new-flaws.html |
| Infected Technology | VMware vRealize Operations (prior to version 8.5.0), VMware Cloud Foundation (versions 3.x and 4.x), and vRealize Suite Lifecycle Manager (version 8.x) |
| Recommendation | Apply all the patches and updates |
| CVE-ID | CVE-2021-22022 (CVSS score: 4.4)<br>CVE-2021-22023 (CVSS score: 6.6)<br>CVE-2021-22024 (CVSS score: 7.5)<br>CVE-2021-22025 (CVSS score: 8.6)<br>CVE-2021-22026 (CVSS score: 7.5)<br>CVE-2021-22027 (CVSS score: 7.5) |

| Critical Cosmos Database Flaw Affected Thousands of Microsoft Azure Customers | |
|---|---|
| **Description** | |
| News about the now-fixed Azure Cosmos database vulnerability has been revealed by the cloud infrastructure security company, Wiz. Dubbed ans ChaosDB, the vulnerability could be exploited to allow any Azure user full admin access with read, write, and delete privileges to other customers' database instances without any authorization. | |
| Source | https://thehackernews.com/2021/08/critical-cosmos-database-flaw-affected.html |
| Infected Technology | Microsoft's Cosmos DB |
| Recommendation | Regenerate Cosmos DB Primary Keys<br>Review all past Cosmos DB account activities<br>Keep all the patches up to date |

F5 Releases critical Security Patch for BIG-IP and Big-IQ Devices

| **Description** | |
|---|---|
| F5 has released fixes for numerous new vulnerabilities affecting BIG -IP and BIG -IQ devices that may allow attackers to read arbitrary files, escalate privileges, and execute JavaScript code, among other things. Of the 29 bugs addressed, 13 are high-severity flaws, 15 are rated medium, and one is rated low in severity. An authorized attacker with access to the Configuration utility can use this vulnerability to run arbitrary system commands, create or remove files, and deactivate services. This flaw has the potential to undermine the entire system. | |
| Source | https://support.f5.com/csp/article/K50974556 |
| Infected Technology | Big IP and Big IQ |
| Recommendation | Update the latest available patch |
| CVE-ID | CVE-2021-23024, CVE-2021-23026, CVE-2021-23027, CVE-2021-23028, CVE-2021-23029, CVE-2021-23030, CVE-2021-23031, CVE-2021-23032, CVE-2021-23033, CVE-2021-23034, CVE-23035, CVE-23036, CVE-23037 |

Flaws found in Opensource elFinder File Manager

| **Description** | |
|---|---|
| Unauthenticated attackers might use critical vulnerabilities in elFinder, the popular opensource web file organizer, to execute arbitrary PHP code on servers hosting elFinder's back-end PHP connector. elFinder, a JavaScriptbased file manager, is used in conjunction with content management systems and frameworks to handle local and remote files. Security researchers have documented five vulnerability chains that combine otherwise “innocuous bugs” to forge exploit chains capable of seizing control of servers. | |
| Source | https://blog.sonarsource.com/elfinder-case-study-of-web-file-manager-vulnerabilities |
| Infected Technology | elFinder File Manager |
| Recommendation | Update the latest available patch |

Kaseya Issues Patches for Two New 0-Day Flaws Affecting Unitrends Servers

| **Description** | |
|---|---|
| Kaseya, a U.S. technology firm has released patches addressing two zero-day vulnerabilities that affected its Unitrends enterprise backup and continuity solution which could potentially lead to privilege escalation and authenticated remote code execution. The vulnerabilities were found by security researchers at the Dutch Institute for Vulnerability Disclosure (DIVD).<br>Kaseya released Unitrends version 10.5.5-2 on August 12 to patch the two server vulnerabilities, but it's still working on a fix for a third unauthenticated remote code execution flaw impacting the client. The company has published firewall rules that can be applied to filter traffic to and from the client and mitigate any risk associated with the flaw. As an additional precaution, it's recommended not to leave the servers accessible over the internet | |
| Source | https://thehackernews.com/2021/08/kaseya-issues-patches-for-two-new-0-day.html |
| Infected Technology | Kaseya UNITRENDS servers |
| Recommendation | Patch vulnerable servers and apply client mitigations<br>https://support.unitrends.com/hc/en-us/articles/360013264518 |

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**

# OUR SERVICES

Our services as information security company includes:

- INFORMATION SECURITY AUDIT
- VULNERABILITY ASSESSMENT
- PENETRATION TESTING
- MANAGED/CO.MANAGED SOC
- INCIDENT RESPONSE
- THREAT ANALYSIS
- SERVER HARDENING
- CYBER SECURITY CONSULTANT
- INFORMATION SECURITY TRAINING

CryptoGen Nepal

https://www.facebook.com/CryptoGenNepal/
https://twitter.com/CryptoGenNepal
https://www.instagram.com/CryptoGenNepal/