

# November 7, 2022

## INFOSEC WEEKLY

#MADE4SECURITY

- OpenSSL Releases Patch for 2 New High-Severity Vulnerabilities.
- Microsoft fixes critical RCE flaw affecting Azure Cosmos DB
- Multiple Vulnerabilities Reported in Checkmk IT Infrastructures Monitoring Software
- Cisco addressed several high-severity flaws in its products
- VMware Warns of Exploit for Recent NSX-V Vulnerability.



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.

---

## OpenSSL Releases Patch for 2 New High-Severity Vulnerabilities.

### Description

The OpenSSL project has rolled out fixes to contain two high-severity flaws in its widely used cryptography library that could result in a denial-of-service (DoS) and remote code execution. The issues, tracked as CVE-2022-3602 and CVE-2022-3786, have been described as buffer overrun vulnerabilities that can be triggered during X.509 certificate verification by supplying a specially crafted email address. OpenSSL is an open-source implementation of the SSL and TLS protocols used for secure communication and is baked into several operating systems and a wide range of software. Versions 3.0.0 through 3.0.6 of the libraries are affected by the new flaws, which has been remediated in version 3.0.7. It's worth noting that the commonly deployed OpenSSL 1.x versions are not vulnerable. While CVE-2022-3602 was initially treated as a Critical vulnerability, its severity has since been downgraded to High, citing stack overflow protections in modern platforms. Security researchers Polar Bear and Viktor Dukhovni have been credited with reporting CVE-2022-3602 and CVE-2022-3786 on October 17 and 18, 2022.

Source	<a href="https://thehackernews.com/2022/11/just-in-openssl-releases-patch-for-2.html">https://thehackernews.com/2022/11/just-in-openssl-releases-patch-for-2.html</a>
--------	---

Infected Technology	Open SSL/TSL Protocol
---------------------	-----------------------

Recommendation	Update to the latest version.
----------------	-------------------------------

CVE_ID	CVE-2022-3602 CVE-2022-3786
--------	--------------------------------

---

---

## Microsoft fixes critical RCE flaw affecting Azure Cosmos DB

### Description

A critical vulnerability affecting Azure Cosmos DB has been found by Orca Security Analysts that allowed unauthenticated read and write access to containers. The security issue was detected in Azure Cosmos DB built-in Jupyter Notebooks that integrate into the Azure portal and Azure Cosmos DB accounts for querying, analyzing, and visualizing NoSQL data and results easier. The vulnerability is also known as as CosMiss. The Orca security discovered that Cosmos DB Jupyter notebooks lacked authentication checks that prevented unauthorized access, and even modify a container.

Source	<a href="https://www.bleepingcomputer.com/news/security/microsoft-fixes-critical-rce-flaw-affecting-azure-cosmos-db/">https://www.bleepingcomputer.com/news/security/microsoft-fixes-critical-rce-flaw-affecting-azure-cosmos-db/</a>
--------	---

Infected Technology	Azure Cosmos DB
---------------------	-----------------

Recommendation	The fixes of this vulnerability have taken place on server side, so users don't need to take action to mitigate it.
----------------	---

---

## Multiple Vulnerabilities Reported in Checkmk IT Infrastructures Monitoring Software

### Description

Multiple vulnerabilities in Checkmk IT Infrastructures monitoring software have been reported, which could be chained together by an unauthenticated, remote attacker to completely take over affected servers. An unauthenticated, remote attacker can exploit these vulnerabilities to obtain code execution on a server running Checkmk versions 2.1.0p10 and lower. The vulnerabilities are command injection flaws, arbitrary file read flaws, command injection flaw, and server-side request forgery flaws.

Source <https://thehackernews.com/2022/11/multiple-vulnerabilities-reported-in.html>

Infected Technology Checkmk

Recommendation Update to the latest version

---

## Cisco addressed several high-severity flaws in its products

### Description

The IT giant has fixed the cross-site request forgery (CSRF) hole that affects the Identity Services Engine, which is the most serious vulnerability (ISE). A remote, unauthenticated attacker can take advantage of the flaw to command arbitrary operations on an affected device. The web-based administration interface of an impacted device's inadequate CSRF safeguards are the main cause of the problem. A cross-site request forgery (CSRF) attack might be launched against an affected device by an unauthenticated, remote attacker. The web-based administration interface of a vulnerable device has weak CSRF safeguards, which is the cause of this vulnerability. An attacker could be able to leverage the target user's rights to carry out arbitrary operations on the harmed device.

Source [https://securityaffairs.co/wordpress/138068/security/cisco-addressed-multiple-flaws.html?web\\_view=true](https://securityaffairs.co/wordpress/138068/security/cisco-addressed-multiple-flaws.html?web_view=true)

Infected Technology Cisco products

Recommendation Update to the latest version.

CVE\_ID CVE-2022-20961

---

---

## VMware Warns of Exploit for Recent NSX-V Vulnerability.

### Description

VMware over the weekend warned of the existence of a public exploit targeting a recently addressed critical remote code execution (RCE) vulnerability in NSX Data Center for vSphere (NSX-V). Last week, VMware announced the availability of patches for CVE-2021-39144 (CVSS score of 9.8), an RCE flaw via the open-source library XStream, warning that it could allow a remote attacker to execute arbitrary code in the context of 'root' on the appliance. Over the weekend, VMware updated its advisory on CVE-2021-39144 to warn that an exploit targeting this vulnerability already exists. "VMware has confirmed exploit code leveraging CVE-2021-39144 against VCF (NSX-V) has been published," the company says. In an accompanying FAQ, VMware warns that successful exploitation of this vulnerability could allow a malicious actor who has network access to the NSX-V Manager to take over the appliance.

Source	<a href="https://www.securityweek.com/vmware-warns-exploit-recent-nsx-v-vulnerability">https://www.securityweek.com/vmware-warns-exploit-recent-nsx-v-vulnerability</a>
--------	---

Infected Technology	VMware vSphere (NSX-V)
---------------------	------------------------

Recommendation	Update to the latest version and look for signs of exploit closely.
----------------	---

CVE_ID	CVE-2021-39144
--------	----------------

---

For any queries/recommendations:

Contact us: [whois@cryptogennepal.com](mailto: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/>