August 1, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- LibreOffice addresses security issues with macros passwords
- Critical Atlassian Confluence Vulnerability Under Active Exploitation
- Three critical vulnerabilities patched by CISCO in Nexus Dashboard
- Microsoft Adds Default Protection Against RDP Brute-Force Attacks in Windows 11
- LibreOffice Releases Software Update to Patch 3 New Vulnerabilities.

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.

LibreOffice addresses security issues with macros, passwords

Description	
A security update has been released to address several security vulnerabilities related to the execution of macros and the protection of web passwords. There are total fixes of three vulnerabilities where first vulnerability allows macro code to run on the target device even if the certificate used to sign the macro doesn't match the entries in the user's configuration database, the second issues was of poor encoding of the master key that stores passwords for web connections in the user's configuration database and the third flaw allows attackers with access to the user's configuration data to retrieve passwords for web connections without knowing the master password.	
Source	https://www.bleepingcomputer.com/news/security/libreoffice-addresses-security-issues-with-macros-passwords/
Infected Technology	LibreOffice
Recommendation	Update to latest version
CVE_ID	CVE-2022-26305, CVE-2022-26307, CVE-2022-2036

Critical Atlassian Confluence Vulnerability Under Active Exploitation

Description	
The flaw is now actively being used in the wild for the Confluence software for Confluence Server and Confluence Data Center. concerns the app's usage of a hard-coded password that a remote, unauthenticated attacker may use to obtain full access to all Confluence pages. Given the significant importance of Confluence for attackers who frequently take advantage of Confluence vulnerabilities to carry out ransomware attacks, monitor exploitation after the hard-coded passwords were disclosed. Only when the Questions for Confluence app is activated does the bug occur. However, since the generated account is not immediately deleted after the Questions for Confluence program has been uninstalled, doing so does not fix the problem. The development also occurs in the wake of Palo Alto Networks' discovery that threat actors begin looking for weak endpoints within 15 minutes following the public announcement of a new security defect in its 2022 Unit 42 Incident Response Report.	
Source	https://thehackernews.com/2022/07/latest-critical-atlassian-confluence.html
Infected Technology	Confluence Server, Confluence Data Center
Recommendation	Update to the latest version (2.7.38 and 3.0.5).
CVE_ID	CVE-2022-26138

Three critical vulnerabilities patched by CISCO in Nexus Dashboard

Description	
Cisco released patches for one critical and two high severity vulnerabilities that could be leveraged by attackers to execute arbitrary code as root, deploy containers and perform cross site scripting (XSS). The most severe, is tracked as CVE-2022-20857 (CVSS 9,8), enables the attacker to perform remote code execution by accessing a vulnerable API. Another flaw, tracked as CVE-2022-20861 (CVSS 8.8) is a CRSF bug that existing the web UI running the management network. Finally, the flaw tracked as CVE-2022-20858 (CVSS 8.2) exposes the services responsible for managing container images for both management and data networks.	
Source	https://portswigger.net/daily-swig/cisco-patches-dangerous-bug-trio-in-nexus-dashboard/
Infected Technology	Cisco Nexus Dashboard – 1.1, 2.0, 2.1, and 2.2
Recommendation	Update and apply the latest patch.
CVE_ID	CVE-2022-20857, CVE-2022-20857, CVE-2022-20861

Microsoft Adds Default Protection Against RDP Brute-Force Attacks in Windows 11

Description	
As part of the most recent releases of the Windows 11 operating system, Microsoft is now taking measures to thwart Remote Desktop Protocol (RDP) brute-force assaults to raise the security bar in response to the changing threat landscape. To that aim, the default setting for Windows 11 builds, namely Insider Preview versions 22528.1000 and newer, locks accounts automatically after 10 unsuccessful sign-in attempts for a period of ten minutes. It's worth pointing out that while this account lockout setting is already incorporated in Windows 10, it's not enabled by default. The feature, which follows the company's decision to resume blocking of Visual Basic Application (VBA) macros for Office documents, is also expected to be backported to older versions of Windows and Windows Server.	
Source	https://thehackernews.com/2022/07/microsoft-adds-default-protection.html
Infected Technology	Windows 10, 11 version below 22528.1000
Recommendation	Upgrade to Latest Windows 11 Version (22528.1000 and newer)

LibreOffice Releases Software Update to Patch 3 New Vulnerabilities.

Description	
LibreOffice's developers have released security upgrades to address three security flaws in the program, one of which might be used to execute arbitrary code on vulnerable PCs. When evaluating if a macro is signed by a trustworthy author, the problem has been described as an example of improper certificate validation that allowed malicious code that was bundled inside the macros to execute. "An adversary could therefore create an arbitrary certificate with a serial number and an issuer string identical to a trusted certificate which LibreOffice would present as belonging to the trusted author, potentially leading to the user to execute arbitrary code contained in macros improperly trusted," LibreOffice said in an advisory.	
Source	https://thehackernews.com/2022/07/libreoffice-releases-software-security.html
Infected Technology	LibreOffice
Recommendation	Update to the latest version.
CVE_ID	CVE-2022-26305, CVE-2022-26307, CVE-2021-25636

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