December 14, 2020

INFOSEC WEEKLY

#MADE4SECURITY

1. D-Link routers vulnerable to command injection attack
2. Zero click wormable RCE vulnerability discovered in Microsoft Teams
3. VMWare command injection Vulnerability
4. Zero-day vulnerability in WordPress SMTP plugin
5. QNAP patches QTS vulnerabilities allowing NAS device takeover
6. Sophos fixes SQL injection in their Cyberoam OS
7. Cisco fixes vulnerabilities in Security Manager
8. Security vulnerabilities in widely used Point-Of-Sales terminals
9. Adobe Fixes three critical-Severity Flaws

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.

1. D-Link routers vulnerable to command injection attack

Description

The wireless routers manufactured by networking hardware supplier company D-Link are found vulnerable to a command injection flaw. The wireless routers are at risk of being attacked through a remotely exploitable root command injection as founded by Digital Defense's vulnerability research team (VRT). The root command injection attacks on vulnerable components could give the attacker control of the router. The attacker could intercept or modify the network traffic, denial-of-service condition and launching attacks on other networking assets.

Source	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10195
Infected Technology	DSR-150, DSR-250, DSR-500, DSR-1000AC VPN routers running firmware version 3.14 and 3.17
Recommendation	Security patches will be available in mid-December. Patch the affected system as soon as the patch is released.

2. Zero click wormable RCE vulnerability discovered in Microsoft Teams

Description

As the research done by oskarsve, a security engineer from evolution gaming found a zero-click remote code execution (RCE) bug in Microsoft Teams desktop apps that could have allowed an adversary to execute arbitrary code by merely sending a specially-crafted chat message and compromise a target's system. To achieve this, the attacker can use a cross-site scripting (XSS) flaw present in the Teams @mention functionality and a JavaScript-based RCE payload to post a harmless-looking chat message containing a user mention either in the form of a direct message or to a channel. It results in complete loss of confidentiality and integrity for end users where the attackers can access private chats, files, internal network, private keys and personal data.

Source	https://github.com/oskarsve/ms-teams-rce/blob/main/README.md
Infected Technology	Microsoft Teams
Recommendation	Define a content security rule Enable Context Isolation for Remote Content

3. VMWare command injection Vulnerability

Description

The National Security Agency (NSA) published a cybersecurity advisory indicating they observed Russian state-sponsored actors exploiting a VMware command injection vulnerability (CVE-2020-4006). The vulnerability requires network access to the administrative configurator on port 8443 (though this can be configured to be any port) and a valid password for the configurator admin account. If these conditions exist, a malicious actor could execute commands with unrestricted privileges on the underlying operating system.

Source	https://kb.vmware.com/s/article/81754
Infected Technology	VMware Access®3 20.01 and 20.10 on Linux®4 VMware vIDM®5 3.3.1, 3.3.2 and 3.3.3 on Linux VMware vIDM Connector 3.3.1, 3.3.2, 3.3.3, 19.03 VMware Cloud Foundation®6 4.x VMware vRealize Suite Lifecycle Manager®7 8.x
CVE	CVE-2020-4006
Recommendation	Installing the patch to address the vulnerability for CVE-2020-4006 Implement workaround for Linux-based appliances and windows-based servers

4. Zero-day vulnerability in WordPress SMTP plugin

Description

Hackers are resetting passwords for admin accounts on WordPress sites using zero-day vulnerability in a popular WordPress plugin installed on more than 500,000 sites. The password reset link is recorded in the Easy WP SMTP debug log. All attackers must do is access the debug log after the password reset, grab the reset link, and take over the site's admin account.

Source	https://blog.nintechnet.com/wordpress-easy-wp-smtp-plugin-fixed-zero-day-vulnerability/
Infected Technology	WordPress sites that use Easy WP SMTP plugin
Recommendation	Update Easy WP SMTP plugin to its latest version.

5. QNAP patches QTS vulnerabilities allowing NAS device takeover

Description

QNAP Systems is warning of high-severity flaws that plague its top-selling network attached storage (NAS) devices. If exploited, the most severe of the flaws could allow attackers to remotely take over NAS devices. The list of vulnerabilities addressed by QNAP include XSS and command injection issues. The vulnerabilities are cross-site-scripting flaws that could allow remote attackers to inject malicious code in File Station, to inject malicious code in System Connection Logs, and to inject malicious code in certificate configuration.

Source	https://www.qnap.com/en-us/security-advisory/qsa-20-12
Infected Technology	All QNAP NAS
CVE_ID	CVE-2020-2495, CVE-2020-2496, CVE-2020-2497, CVE-2020-2498, CVE-2020-2493, CVE-2020-2491
Recommendation	Update QNAP to the latest version available.

6. Sophos fixes SQL injection in their Cyberoam OS

Description

Sophos has released a hotfix the Routers and Firewalls lineup for Cyberoam OS. The vulnerability allowed attacker to remotely add account on the device if the administrative interface is allowed in WAN interface. Sophos has been phasing out Cyberoam OS for XG Firewall OS since 2019. Sophos has deployed hotfix to be delivered to vulnerable devices via “Over-the-air Hotfix” feature.

Source	https://support.sophos.com/support/s/article/KB-000040678?language=en_US
Infected Technology	Cyberoam OS version: • Version 10.6.4 and above • Version 10.6.3 MR4 & MR5, 10.6.2 MR1 • All versions prior to and including 10.6.1
CVE_ID	CVE-2020-29574
Recommendation	Verify if the released Hotfix has been applied

7. Cisco fixes vulnerabilities in Security Manager

Description

Cisco has released a patch to address multiple vulnerabilities in Cisco Security Manager which allowed unauthenticated attacker to execute remote code in the platform. The vulnerabilities affect Cisco devices including Cisco ASA, Switches and Firewall. The POC exploit has been available for the vulnerabilities since November, however, no public exploitation has been recorded according Cisco.

Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-java-rce-mWJEedcD
Infected Technology	Cisco Security Manager
CVE_ID	CVE-2020-27131
Recommendation	Apply the security update released by OEM

8. Security vulnerabilities in widely used Point-Of-Sales terminals

Description

Verifone and Ingenico, two of the biggest manufacturer of point-of-sales (POS) terminals are found vulnerable to flaws that allow attackers to steal credit card, clone terminals and commit various financial fraud. One of the common flaws in each manufacturer is the use of default password allowing attacker to access service menu and manipulate and change the code on machine to run malicious command. The flaw could also be remotely exploited to execute arbitrary code, cause buffer overflow and control the device to record the data in the devices.

Source	https://www.cyberdlab.com/research-blog/posworld-vulnerabilities-within-ingenico-telium-2-and-verifone-vx-and-mx-series-point-of-sales-terminals
Infected Technology	Verifone VX520, Verifone MX series, and the Ingenico Telium 2 series.
Recommendation	Apply the patch released by OEM Prevent the use of default credentials in your devices

9. Adobe Fixes three critical-Severity Flaws

Description

Adobe Devices has stomped out critical-severity flaws throughout its Adobe Prelude, Adobe Encounter Manager and Adobe Lightroom applications. If exploited, the significant vulnerabilities could guide to arbitrary code execution. The cross-site scripting (XSS) vulnerability in AEM could allow a poor actor to execute arbitrary JavaScript on the victim's browser. Another flaw also exist on AEM , which is blind server-side request forgery occurs when an application can be manipulated to issue a back-end HTTP request to supplied URL but no response in returned in the application's front-end from back-end request leads to sensitive data disclosure.

Source	https://helpx.adobe.com/security/products/experience-manager/apsb20-72.html
Infected Technology	Adobe Experience Manager (AEM) • AEM Cloud Service (CS) • 6.5.6.0 and earlier versions • 6.4.8.2 and earlier versions • 6.3.3.8 and earlier versions • 6.2 SP1-CFP20 and earlier versions AEM Forms add-on • AEM Forms Service Pack 6 add-on package for AEM 6.5.6.0 • AEM Forms add-on package for AEM 6.4 Service Pack 8 Cumulative Fix Pack 2 (6.4.8.2) Adobe Light Room, Adobe Prelude
CVE_ID	CVE-2020-24444, CVE-2020-24445, CVE-2020-24447
Recommendation	Adobe recommend their users to update their installation to the newest available version

10.Apache fixes code execution in Apache Struts 2

Description

Apache Software Foundation has released security update for Struts 2 to address a possible remote code execution. The flaw resides in evaluation of raw user input in tag attribute. Forced OGNL evaluation may result in double evaluation that can lead to remote code execution and security degradation. The flaw is like CVE-2019-0230 whose exploit was released on August.

Source	https://cwiki.apache.org/confluence/display/WW/S2-061
Infected Technology	Struts 2.0.0 - Struts 2.5.25
CVE_ID	CVE-2020-17530
Recommendation	Upgrade to Struts 2.5.26 or greater

11. Google patches critical Wi-Fi and Audio Bugs in Android handsets

Description

Google patched multiple critical security bugs in Android OS. One of patched vulnerability may result in remote code execution which is tied to Android media framework component while nine others are tied to underlying Qualcomm chipsets and accompanying firmware. All patched Qualcomm's bugs were rated 9.8 out of 10 in CVSS score. Several of the critical flaws were identified as buffer-overflow bugs and buffer over-read vulnerabilities. Although the vulnerabilities has been patched by Google in Android, it is upon individual handset manufacturer to release the patch to their customers.

Source	https://source.android.com/security/bulletin/2020-12-0
Infected Technology	Android OS
CVE_ID	CVE-2020-0458, CVE-2020-11225, CVE-2020-11137
Recommendation	Apply the security update once released by device manufacturer

12. PLEASE_READ_ME Ransomware attacks 85K MySQL Server

Description

Researchers are warning about an active ransomware campaign that's targeting MySQL database servers. The ransomware, called PLEASE_READ_ME, has thus far breached at least 85,000 servers worldwide – and has posted at least 250,000 stolen databases on a website for sale. The attack starts with a password brute-force on the MySQL service. Once successful, the attacker runs a sequence of queries in the database, gathering data on existing tables and users. Researchers believe that the attackers behind this campaign have made at least $25,000 in the first 10 months of the year.

Source	https://www.guardicore.com/labs/please-read-me-opportunistic-ransomware-devastating-mysql-servers/
Infected Technology	MySQL Servers
Recommendation	Use a strong password combination on publicly facing MySQL servers.

13. Cisco reissues patches for bugs in Jabber Video Conferencing Software

Description

Cisco has once again patched the four critical bugs in the Jabber video conferencing and messaging app. The issue was reported by Watchcom in which the users were susceptible to remove attacks. The successful exploitation of these vulnerabilities could allow an authenticated remote attacker to execute arbitrary code on the target system by sending a fabricated chat message to an individual or a group. Three out of four vulnerabilities reported have not been sufficiently mitigated. One of the non-mitigated vulnerability is worm-able hence, can automatically spread malware to other systems by disguising in a chat message. The vulnerabilities are prone to zero-click cross-site scripting (XSS), command injection flaw and file transfer message manipulation.

Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-ZktzjpgO
Infected Technology	Cisco Jabber Client 12.1 – 12.9
CVE	CVE-2020-26085, CVE-2020-27132, CVE-2020-27127
Recommendation	Update Jabber to the latest version. For organization, disable communication through Cisco Jabber until all employees have installed the update.

14. Microsoft Releases Windows Update to Fix 58 Security Flaws

Description

On Tuesday, Microsoft has released fixes for 58 newly discovered security flaws spanning as many as 11 products and services as part of its final patch Tuesday of 2020. The December security release addresses issues in Microsoft Windows, Edge browser, ChakraCore, Microsoft Office, Exchange Server, Azure DevOps, Microsoft Dynamics, Visual Studio, Azure SDK, and Azure Sphere.

Source	https://msrc.microsoft.com/update-guide/releaseNote/2020-Dec
Infected Technology	Windows Operating Systems
CVE	CVE-2020-17132, CVE-2020-17118, CVE-2020-17121 CVE-2020-17123, CVE-2020-17095, CVE-2020-16996
Recommendation	Update windows OS to its latest version.

15. Adrozek malware hijacking popular web browsers

Description

"Adrozek" called by the Microsoft 365 Defender Research Team employs an "expansive dynamic attacker infrastructure" that includes 159 unique domains, each hosting an average of 17,300 unique URLs which host more than 15,300 unique malware sample. Once installed on a target system by drive-by downloads, Adrozek makes multiple changes on the browser settings and security controls to install malicious add-ons that hide as a genuine extension. The malware disables the integrity checks on modern browsers to allow attackers to avoid security defense to inject unauthorized advertisements on top of legitimate ads and drive traffic to the fraud ad pages hence, gaining revenue. On Firefox, credential theft is executed, and data is exfiltrated to the attacker-controlled server.

Source	https://www.microsoft.com/security/blog/2020/12/10/widespread-malware-campaign-seeks-to-silently-inject-ads-into-search-results-affects-multiple-browsers/
Infected Technology	Microsoft Edge, Google Chrome, Yandex Browser, Mozilla Firefox on Windows
Recommendation	Do not download applications from untrusted sources

For any queries/recommendations:

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