

April 12 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Cisco fixes bug allowing RCE with root privileges
- Google Patches Critical Code Execution Vulnerability in Android
- Critical SAP Applications Are Under Active Attack
- Cisco will not patch critical RCE flaws affecting end-of-life routers
- VMware Patches Critical Flaw in Carbon Black Cloud Workload
- WhatsApp-based wormable Android malware spotted on the Google Play Store
- Apple Mail Zero-Click Security Vulnerability Allows Email Snooping
- Bug allows attackers to hijack Windows time sync software used to track security incidents



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. Cisco fixes bug allowing RCE with root privileges

Description

Cisco has introduced security updates to address critical pre-authentication remote code execution (RCE) vulnerability. The vulnerability had affected SD-WAN vManage Software's remote management component. The company has identified and fixed two high-severity security vulnerabilities that could allow malicious actors to obtain root privileges if successfully exploited. The successful exploitation was possible if the attacker sends a crafted connection request to the vulnerable component causing a buffer overflow condition. This resulted in allowing an attacker to execute arbitrary commands on the affected operating system with root privileges.

Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-YuTVWqy
Infected Technology	Cisco SD-WAN vManage releases 20.4 and earlier
CVE ID	CVE-2021-1137, CVE-2021-1479, CVE-2021-1480
Recommendation	Consider installing the security patches provided by cisco.

2. Google Patches Critical Code Execution Vulnerability in Android

Description

There are more than 30 vulnerabilities in mobile operating system, according to the Android security bulletin published by Google this week. It includes a remote code execution flaw in the System component affecting Android 10 and 11. The code execution vulnerability is deemed critical severity and was patched as part of the 2021-04-01 security patch level. This vulnerability could enable a remote attacker using a specially crafted file to execute arbitrary code within the context of a privileged process.

Source	https://source.android.com/security/bulletin/2021-04-01
Infected Technology	Android 10 and 11
CVE ID	CVE-2021-0430
Recommendation	Consider updating your android devices to their latest version.

3. Critical SAP Applications Are Under Active Attack

Description	
-------------	--

Cyber attackers are actively setting their sights on unsecured SAP applications to steal information and sabotage critical processes. Cybersecurity firm Onapsis and SAP said in a joint report that the observed exploitation could lead in many cases to full control of the unsecured SAP application, bypassing common security and compliance controls, and enabling attackers to steal sensitive information, perform financial fraud or disrupt mission-critical business processes by deploying ransomware or stopping operations. Onapsis report outlines weaponization of SAP vulnerabilities in less than 72 hours from the release of patches, with new unprotected SAP applications provisioned in cloud environments being discovered and compromised in less than 3 hours.	
---	--

Source	https://thehackernews.com/2021/04/watch-out-mission-critical-sap.html
--------	---

Infected Technology SAP Applications such as

- enterprise resource planning (ERP),
- supply chain management (SCM),
- human capital management (HCM),
- product lifecycle management (PLM),
- customer relationship management (CRM)

CVE ID	CVE-2010-5326, CVE-2016-3976, CVE-2016-9563 CVE-2018-2380, CVE-2020-6207, CVE-2020-6287
--------	--

Recommendation	Consider updating SAP applications to its latest version.
----------------	---

4. Cisco will not patch critical RCE flaws affecting end-of-life routers

Description

Cisco System has stated that it does not plan to fix a critical security vulnerability affecting the Small Business routers lineup. Cisco has urged users and clients to replace the device. The flaw present in these routers is due to improper validation of user-supplied input in a web-based management interface. The exploitation of this error could enable malicious actors to send a specially crafted HTTP request to the target and achieve remote code execution. The successful exploitation could allow an attacker to execute an arbitrary command as the root user. Cisco has stated that the Small business routers have entered the end-of-life process.

Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm
Infected Technology	Cisco Small Business RV110W, RV130, RV130 and RV215W
CVE ID	CVE-2021-1459
Recommendation	Consider finding alternatives for Cisco Small Business RV132W, RV160, or RV160W routers

5. VMware Patches Critical Flaw in Carbon Black Cloud Workload

Description

According to a warning from a security researcher who discovered the bug, a critical vulnerability recently addressed in the VMware Carbon Black Cloud Workload could be abused to execute code on a vulnerable server. The recently addressed vulnerability resides in the administrative interface for the appliance and exists because attackers could bypass authentication through manipulation of a URL on the interface. According to VMware, a malicious actor with network access to the administrative interface of the VMware Carbon Black Cloud Workload appliance may be able to obtain a valid authentication token, granting access to the administration API of the appliance.

Source	https://www.vmware.com/security/advisories/VMSA-2021-0005.html
Infected Technology	VMware Carbon Black Cloud Workload appliance
CVE ID	CVE-2021-21982
Recommendation	Consider applying the patches released by VMware.

6. WhatsApp-based wormable Android malware spotted on the Google Play Store

Description

Malware has been discovered on Google Play, hidden in a fake application called 'FlixOnline' that is capable of spreading itself via users' WhatsApp messages. If the user downloaded the fake application and unwittingly granted the malware the appropriate permissions, the malware is capable of automatically replying to the victim's incoming WhatsApp messages with a payload received from a command-and-control (C&C) server. Besides masquerading as a Netflix app, the malicious "FlixOnline" app also requests intrusive permissions that allow it to create fake Login screens for other apps, to steal credentials and gain access to all notifications received on the device, using it to hide WhatsApp notifications from the user and automatically reply with a specially-crafted payload received from the C&C server.

Source	https://research.checkpoint.com/2021/new-wormable-android-malware-spreads-by-creating-auto-replies-to-messages-in-whatsapp/
--------	---

Infected Technology	FlixOnline Android Application
---------------------	--------------------------------

Recommendation	Consider not using the FlixOnline app.
----------------	--

7. Apple Mail Zero-Click Security Vulnerability Allows Email Snooping

Description

A zero-click security vulnerability in Apple's macOS Mail would allow a cyber attacker to add or modify any arbitrary file inside Mail's sandbox environment, leading to a range of attack types. The exploitation of the bug could lead to unauthorized disclosure of sensitive information to a third party; the ability to modify a victim's Mail configuration, including mail redirects which enables takeover of victim's other accounts via password resets; and the ability to change the victim's configuration so that the attack can propagate to correspondents in a worm-like fashion. To exploit the bug, a cyberattacker could email two ZIP files as attachments to the victim, according to the analysis. When a user receives the email, the Mail app will parse it to find any attachments with an x-mac-auto-archive=yes header in place. Mail will then automatically unpack those files.

Source	https://mikko-kenttala.medium.com/zero-click-vulnerability-in-apples-macos-mail-59e0c14b106c
--------	---

Infected Technology	Apple's OS Mail service
---------------------	-------------------------

CVE ID	CVE-2020-9922
--------	---------------

Recommendation	Consider applying the patches provided by Apple
----------------	---

8. Bug allows attackers to hijack Windows time sync software used to track security incidents

Description

Researchers at GRIMM on Tuesday said that they found a remote code execution (RCE) vulnerability that can let attackers hijack the update process of a popular Windows time synchronization software product – Greyware’s Domain Time II - by exploiting a man-on-the-side (MotS) vulnerability. An attacker can trick a user into downloading and executing an attacker-controlled payload under the guise of a routine software update. Since the attack is performed in the context of a MotS, the attacker cannot manipulate the data exchanged between a local install and the update server. However, the attacker can send out their responses and ‘race’ the legitimate traffic. If the attacker wins the ‘race’, the local install will open a browser window and drive it to a URL supplied by the attacker.

Source	https://blog.grimm-co.com/2021/04/time-for-upgrade.html
--------	---

Infected Technology	Domain Time II versions 5.2.x (current releases), 5.1.x (starting from 2010), and 4.1.x (starting from 2007) from 5.2.b.20210103 to at least 4.1.b.20070308
---------------------	--

Recommendation	Consider upgrading to the latest patched version.
----------------	---

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/>