May 10
2021

INFOSEC WEEKLY

#MADE4SECURITY

- VMware fixed RCE bug in vRealize Business for Cloud
- Foxit Reader bug lets attackers run malicious code via PDFs
- Six Unpatched Flaws Disclosed in Remote Mouse App for Android and iOS
- Apple reports 2 iOS 0-days that let hackers compromise fully patched devices
- Cisco fixes SD-WAN vManage and HyperFlex Software flaws
- Anti-Spam WordPress Plugin Could Expose Website User Data
- Android May 2021 Update Out, Fixes Over 40 vulnerabilities
- Dell patches 12-year-old driver vulnerability impacting millions of PCs

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. VMware fixed RCE bug in vRealize Business for Cloud

Description

VMware has released security updates to rectify critical security vulnerability in the vRealize Business for Cloud products. The vulnerability allowed attackers to perform and execute malicious code remotely to affect the vulnerable endpoint. vRealize Business for Cloud is an automated solution for cloud business management that provides cloud planning, budgeting, and cost analysis tools. The attackers can exploit the endpoint flaw within by using the management interface (VAMI) upgrade API. The RCE vulnerability could be exploited remotely via low complexity attacks. The attacks did not require any authentication or user interaction.

Source	https://www.vmware.com/security/advisories/VMSA-2021-0007.html
Infected Technology	VMware vRealize Business for Cloud
CVE ID	CVE-2021-21984
Recommendation	Install the latest VMware vRealize Business for Cloud 7.6.0 to patch the vulnerability.

2. Foxit Reader bug lets attackers run malicious code via PDFs

Description

Foxit Software, the company behind the highly popular Foxit Reader, has published security updates to fix a high severity remote code execution (RCE) vulnerability affecting the PDF reader. This security flaw results from a “Use After Free” bug found in the V8 JavaScript engine used by Foxit Reader to display dynamic forms and interactive document elements. This security flaw is caused by how the Foxit Reader application and browser extensions handle certain annotation types, which attackers can abuse to craft malicious PDFs that will allow them to run arbitrary code via precise memory control.

Source	https://www.foxitsoftware.com/support/security-bulletins.html
Infected Technology	Foxit Reader version <= 10.1.3.37598
CVE ID	CVE-2021-21822
Recommendation	Consider upgrading to the latest Foxit Reader version 10.1.4.37851

3. Six Unpatched Flaws Disclosed in Remote Mouse App for Android and iOS

Description	
As many as six zero-days have been uncovered in an application called Remote Mouse, allowing a remote attacker to achieve full code execution without any user interaction. The unpatched flaws, collectively named Mouse Trap, were disclosed on Wednesday by security researcher Axel Persinger, who said, "It's clear that this application is very vulnerable and puts users at risk with bad authentication mechanisms, lack of encryption, and poor default configuration." This issue could allow an adversary to intercept a user's hashed password, rendering them susceptible to rainbow table attacks and even replay the commands sent to the computer.	
Source	https://axelp.io/MouseTrap
Infected Technology	Remote Mouse App (Android and iOS)
CVE ID	CVE-2021-27569, CVE-2021-27570, CVE-2021-27571, CVE-2021-27572, CVE-2021-27573, CVE-2021-27574
Recommendation	Consider using alternatives of Remote Mouse App until the patch gets released.

4. Apple reports 2 iOS 0-days that let hackers compromise fully patched devices

Description	
After the release of IOS version 14.0, the company has released a new update to patch two zero-days that allowed attackers to execute malicious code on fully up-to-date devices. The newly released version 14.5.1 fixes problems with a bug in the newly released App Tracking Transparency feature rolled out in the previous version. Both vulnerabilities reside in Webkit, a browser engine that renders Web content in Safari, Mail, App Store, and other select apps running on iOS, macOS, and Linux.	
Source	https://support.apple.com/en-us/HT212335
Infected Technology	iOS
CVE ID	CVE-2021-30663 and CVE-2021-30665
Recommendation	Update the iOS to the latest version

5. Cisco fixes SD-WAN vManage and HyperFlex Software flaws

Description	
Cisco has released software updates that address critical vulnerabilities residing in HyperFlex HX and SD-WAN vManage Software. The identified vulnerabilities could allow attackers to perform command injection, arbitrary code attacks to gain sensitive information of the endpoint. The HyperFlex HX command injection was present as a result of insufficient validation of the user-data input in web-based management interfaces. The flaws allowed attackers to send a crafted request to the web interface and enable an unauthenticated remote-based attacker to perform command injection in the vulnerable endpoint. The glitches present in SD-WAN vManage Software also allowed an authenticated remote-based attacker to execute arbitrary codes, and gain access to sensitive information. The vulnerability allowed local authenticated attackers to gain escalated privileges or gain unauthorized access to the application.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR
Infected Technology	Cisco HyperFlex HX and SD-WAN vManage
CVE ID	CVE-2021-1497, CVE-2021-1498, CVE-2021-1275 CVE-2021-1468, CVE-2021-1505, CVE-2021-1506 CVE-2021-1508
Recommendation	Update to the latest version released by Cisco.

6. Anti-Spam WordPress Plugin Could Expose Website User Data

Description

An SQL injection vulnerability discovered in a WordPress plugin called “Spam protection, AntiSpam, FireWall by CleanTalk” could expose user emails, passwords, credit card data, and other sensitive information to an unauthenticated attacker. It is installed on more than 1,00,000 sites and is mainly used to weed out spam and trash comments on website discussion boards. According to Wordfence, the issue arises due to its filtering mechanism. It maintains a blocklist and tracks the behavior of different IP addresses, including the user-agent string that browsers send to identify themselves. Unfortunately, the update_log function in lib/Cleantalk/ApbctWP/Firewall/SFW.php, which was used to insert records of these requests into the database, failed to use a prepared SQL statement.

Source	https://www.wordfence.com/blog/2021/05/sql-injection-vulnerability-patched-in-cleantalk-antispam-plugin/
Infected Technology	Spam protection, AntiSpam, FireWall by CleanTalk
CVE ID	CVE-2021-24295
Recommendation	Consider updating the plugin to its latest version.

7. Android May 2021 Update Out, Fixes Over 40 vulnerabilities

Description

Googles’ Android operating system update for May 2021 addresses a total of 42 vulnerabilities, four of which are marked as critical severity. The new security patch fixes three main critical flaws which were identified in the System component. All these three security breaches could be exploited to run arbitrary code on a vulnerable Android device. The fourth vulnerability entails that a malicious local app can bypass user interaction requirements and, therefore, gain access to additional permission. Besides these critical flaws, Android OS has been patched for five other high-severity vulnerabilities. Three of these are related to privilege advancement, while the other two are associated with leaking information.

Source	https://source.android.com/security/bulletin/2021-05-01
Infected Technology	Google’s Android Operating Systems
CVE ID	CVE-2021-0472, CVE-2021-0485, CVE-2021-0487, CVE 2021-0467
Recommendation	Consider updating your Android phones.

8. Dell patches 12-year-old driver vulnerability impacting millions of PCs	
Description	
Hundreds of millions of Dell desktops, laptops, notebooks, and tablets will need to update their Dell DBUtil driver to fix a 12-year-old vulnerability that exposes systems to attacks. The bug impacts the DBUtil Dell BIOS driver that allows the OS and system apps to interact with the computer's BIOS and hardware. The vulnerability in this driver cannot be exploited over the internet to gain access to unpatched systems remotely. Instead, threat actors who gained initial access to a computer, even to a low-level account, could abuse this bug to take full control over the compromised PC leading to a successful privilege escalation.	
Source	https://www.dell.com/support/kbdoc/en-in/000186019/dsa-2021-088-dell-client-platform-security-update-for-dell-driver-insufficient-access-control-vulnerability
Infected Technology	Dell BIOS driver – DBUtil (version 2.3)
CVE ID	CVE-2021-21551
Recommendation	• Consider installing a remediated package containing BIOS, Thunderbolt firmware, TPM firmware, or dock firmware. • Consider updating Dell Command Update, Dell Update, or Alienware Update. • Consider installing the latest version of Dell System Inventory Agent or Dell Platform Tags.

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/