July 20,
2020

INFOSEC WEEKLY

#MADE4SECURITY

- High-Profile Twitter Account Hacked in CryptoScam
- New Android Malware Steals Passwords for Non-Banking App
- SIGRed: Windows DNS Server Remote Code Execution
- A new flaw in Zoom could have let fraudsters mimic organizations
- POC exploit for SAP RECON released
- Adobe issued critical security patch for multiple software
- Brazilian Banking Trojan
- 36 new vulnerabilities in Cisco Products, patch available

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. High-Profile Twitter Account Hacked in CryptoScam

Description	
Several high-profile Twitter Account were simultaneously hacked on Wednesday by attackers who used the accounts with millions of followers, to spread a cryptocurrency scam. The account started tweeting out a message promoting a cryptocurrency give away, in which funds sent to a specified bitcoin wallet would return double the amount to the sender. The messages, which were all similar, and all included the same bitcoin wallet address, were seemingly part of an elaborate hack, likely the largest ever seen on Twitter, which has sparked a new investigation into Twitter's Security. Security researchers, however, found that the attackers had fully taken over the victims' accounts, and also changed the email address associated with the account to make it harder for the real user to regain access.	
Source	https://thehackernews.com/2020/07/verified-twitter-hacked.html
Infected Area	Twitter
Recommendation	We advised the public not to fall victim to this scam by sending cryptocurrency or money in relation to this incident.

2. New Android Malware Steals Passwords for Non-Banking App

Description	
Researcher disclosed a new banking malware that targets not only banking apps but also steals 337 non-financial Android applications which includes social networking, dating and cryptocurrency apps. The malware feature is stealing user credentials, intercepting SMS messages, hijacking notifications, and even recording keystrokes from the targeted apps, in addition to being capable of hiding from anti-virus. BlackRock Does the data collection by abusing Android's Accessibility service Privileges, for which it seeks users' permissions under the guise of fake Google updates when it's launched for the first time on the device.	
Source	https://thehackernews.com/2020/07/android-password-hacker.html
Infected Technology	Android Applications
Recommendation	Do not Install the third-party Applications

3. SIGRed: Windows DNS Server Remote Code Execution

Description	
Cyber Security Researcher warned organization to patch their Microsoft Windows Server builds to protect their network against a new highly critical "wormable" Vulnerability that has existed for 17 years long. This could allow an unauthenticated, remote attacker to gain domain administrator privileges over targeted servers and seize complete control of an organization. The bug related to Microsoft Windows DNS, the domain name system service on Windows operating system, and Server Software. The disclosed vulnerability has a severity score of 10 out of 10.	
Source	https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/
Infected Technology	Windows DNS Server 2003 to 2019
Recommendation	We strongly recommend users to patch their affected Windows DNS Servers in order to prevent the exploitation of this vulnerability
CVEs	CVE-2020-1350

4. A new flaw in Zoom could have let fraudsters mimic organizations

Description	
Researchers at CheckPoint disclosed details of a flaw in Zoom that could let attacker mimic an organization, tricking its employees or business partners into revealing personal or other confidential information using social engineering tricks. The vulnerability resides in Zoom's customized URL feature dubbed Vanity URL, aiming to let companies create a custom URL on its subdomain. Attacker can convert normal invitation link to imitate the subdomain of an organization, implying the invitation is from genuine organization. The issue has been disclosed to Zoom Video communications Inc. and security researchers from CheckPoint and Zoom worked together to put additional safeguard for the protection of users	
Source	https://thehackernews.com/2020/07/zoom-vanity-url-vulnerability.html
Infected Technology	Zoom Video Conferencing Platform
Recommendation	Verify the people you are communicating is a legit user Do not disclose confidential information until the receiver is verified

5. Adobe issued critical security patch for multiple software

Description	
Adobe has released 13 new security patches for 5 different widely used application. Four of the vulnerability is rated to be critical while remaining are important. The patches are for Adobe Creative Cloud Desktop Application, Adobe Media Encoder, Adobe Genuine Service, Adobe ColdFusion and Adobe Download Manager. Adobe Creative Cloud Desktop Application version 5.1 is vulnerable to four vulnerabilities which include a critical symlink flaw leading to arbitrary file system write attacks and three others privilege escalation. Adobe Media Encoder contains two critical arbitrary code execution and one important privilege escalation issue affecting Windows and macOS users. Adobe Genuine Service is affected by three privilege escalation issue while Adobe ColdFusion is affected by two privilege escalation that can be carried out by exploiting DLL search-order hijacking. Adobe Download Manager is also vulnerable to arbitrary code execution in the current user through command injection attack.	
Source	https://thehackernews.com/2020/07/adobe-security-patch-july.html
Infected Technology	• Adobe Creative Cloud Desktop Application version 5.1 and earlier for Windows • Adobe Media Encoder version 14.2 and earlier for Windows and macOS • Adobe Genuine Service version 6.6 and earlier for Windows and macOS • Adobe ColdFusion • Adobe Download Manager version 2.0.0.518 for Windows
CVEs	CVE-2020-9682, CVE-2020-9650, CVE-2020-9646, CVE-2020-9688
Recommendation	Update the patch released by Adobe

6. POC exploit for SAP RECON released

Description	
Last week, SAP released patches for a critical NetWeaver AS JAVA remote code execution vulnerability. A proof of concept exploit has been released for the same and active scans are underway to exploit devices. The vulnerability was discovered by Onapsis, RECON (Remotely Exploitable Code on NetWeaver) has a score of 10 out of 10. The vulnerability when exploited allows attacker to gain full access control of the system. The exploit has been released alongside for another directory traversal flaw for the same.	
Source	https://www.bleepingcomputer.com/news/security/poc-exploits-released-for-sap-recon-vulnerabilities-patch-now/
Infected Technology	SAP NetWeaver version 7.30 to 7.50
CVEs	CVE-2020-6287, CVE-2020-6286
Recommendation	Update the patch released by OEM

7. Brazilian Banking Trojan

Description	
Cybersecurity researchers detailed as many as four different families of Brazilian banking trojans that have targeted financial institutions in Brazil, Latin America, and Europe. Collectively Called the “Tetrade” , the malware families which compromising Guildma, Javali, Melcoz, and Grandoreiro have evolved their capacities to function as a backdoor and adopt a variety of obfuscation techniques to hide its malicious activities from security software. yet another Brazilian banking group/operation that has decided to expand its attacks abroad, targeting banks in other countries. This malware families are examples of yet another Brazilian banking group/operation that has decided to expand its attack abroad, targeting banks in other countries.	
Source	https://thehackernews.com/2020/07/brazilian-banking-trojan.html
Infected Areas	Banking

8. 36 new vulnerabilities in Cisco Products, patch available

Description	
Cisco has released a security update that acknowledges 34 vulnerabilities including five critical. One of the critical bugs with CVSS score of 9.8 impacts the Telnet service in Cisco's VPN router using default, static password which can lead to full remote hijack of a device. Three other critical vulnerability in web management portal allowed arbitrary code execution as root/administrative user. Fifth vulnerability present in Cisco Prime License Manager (PLM) is caused due to improper input validation that could be abused to gain administrative-level privilege escalation if username is known.	
Source	https://www.zdnet.com/article/cisco-releases-fixes-for-critical-vpn-router-vulnerabilities/
Infected Technology	Cisco products
CVEs	CVE-2020-3330, CVE-2020-3323, CVE-2020-3144, CVE-2020-3331, CVE-2020-3140, CVE-2020-11896, CVE-2020-11897, CVE-2020-3381, CVE-2020-3387, CVE-2020-3385, CVE-2020-3351, CVE-2020-3180, CVE-2020-3357, CVE-2020-3358, CVE-2020-3145, CVE-2020-3146, CVE-2020-3369, CVE-2020-3332, CVE-2020-3388, CVE-2020-3468, CVE-2020-3379, CVE-2020-3406, CVE-2020-3405, CVE-2020-3437, CVE-2020-3401, CVE-2020-3450, CVE-2020-3378, CVE-2020-3150, CVE-2020-3372, CVE-2020-3348, CVE-2020-3349, CVE-2020-3380, CVE-2020-3197, CVE-2020-3345, CVE-2019-12644, CVE-2020-3370
Recommendation	Update the patch released by OEM

For any queries/recommendations:

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