June 8, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Proof-of-Concept available for Windows 10 SMBGhost with RCE exploit
- O365 phishing baits remote workers with fake VPN config
- VMware Cloud Director flaw lets hackers take over virtual datacenters
- Fake Ransomware double encrypts victims' file
- Vulnerabilities in SAP's Adaptive Servers
- New USBCulprit espionage tool steal data from Air-gapped computer
- Two New Vulnerabilities in Zoom

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, Trip Advisor, 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 warns about critical flaw in IOS router allowing system compromise

Description

Cisco has disclosed 4 new critical flaws in its router using IOS XE and IOS software. The vulnerability includes CVE-2020-3227, CVE-2020-3205, CVE-2020-3198 and CVE-2020-3258. CVE-2020-3227 has a CVS score of 9.8 which allowed remote attacker to execute Cisco IOx API command without authorization. CVE-2020-3250 is a flaw in Cisco's inter-VM channel in Cisco IOS software for Cisco 809, 829 and 1000 routers which allows attacker to send malicious packet to gain root access to Virtual Device Server (VDS). Other two flaw allows RCE in same devices. Allof the bugs were found by testing team of Cisco and no reports regarding mass exploitation has been released.

Source	https://www.zdnet.com/article/ciscos-warning-critical-flaw-in-ios-routers-allows-complete-system-compromise/
Infected Technology	Cisco IOS XE Software, Cisco 809, 829 and 1000 series router
CVEs	CVE-2020-3227, CVE-2020-3205, CVE-2020-3198, CVE-2020-3258
Recommendation	Update the patch released by Cisco

2. Joomla database leaks personal information

Description

A Joomla database leak has exposed the personal information, including hashed passwords, of 2,700 individuals registered on the Joomla Resources Directory (JRD). The Joomla Resources Directory allows users to find registered service providers to assist in project management, design, and technical support for Joomla. In a security advisory published by Joomla last week, it was disclosed that the details of 2,700 individuals registered on the Joomla Resources Directory (JRD) service were leaked. The leak exposed information such as, Full name, Email, Hashed password, etc.

Source	https://www.bleepingcomputer.com/news/security/joomla-data-breach-leaks-2-700-user-records-via-exposed-backups/
Infected Technology	Joomla
Recommendation	Change your credentials in all platforms if you are utilizing Joomla CMS

3. Two New Vulnerabilities in Zoom

Description	
Two new vulnerabilities in the popular video conferencing software Zoom, has been discovered. These new flaws allow attackers to hack into the systems of group chat participants. Both these vulnerabilities are path traversal vulnerability. Path traversal vulnerability allows an attacker to read arbitrary files on the server that is running an application. The flaws on Zoom can be exploited to write arbitrary files on the systems running vulnerable versions of this software to execute malicious code. Exploitation of these flaws can be done by sending specially crafted messages through the chat feature. The vulnerability (CVE-2020-6109) resides in the way Zoom leverages GIPHY service. Zoom did not check where the GIF was loaded from, which allowed attackers to embed GIFs from a third-party attacker-controlled server. This GIF was cache/store on the recipients' system in a specific folder. Since the application did not sanitize the filenames, this allowed attackers to trick the application into saving malicious files disguised as GIFs to any location on the victim's system. The second vulnerability (CVE-2020-6110) resided in the way Zoom processes code snippets shared through the chat. Zoom has patched both these vulnerabilities in its latest version 4.6.12.	
Source	https://thehackernews.com/2020/06/zoom-video-software-hacking.html
Infected Technology	Zoom: Video Conferencing
Recommendation	Update to the latest version
CVE	CVE-2020-6109, CVE-2020-6110

4. New USBCulprit espionage tool steal data from Air-gapped computer

Description	
Kaspersky has identified a new threat actor named USBCulprit which targets air-gapped systems to extract sensitive data. This tool relies on USB device to reach air-gapped network in client's environment. The malware is capable of scanning paths to search for files with various extensions for documents and exporting itself to connected USB drive. The malware also replicates itself to other USB devices to move laterally in air-gapped network.	
Source	https://thehackernews.com/2020/06/air-gap-malware-usbculprit.html
Infected Technology	USB devices
Recommendation	Use endpoint security solutions

5. Vulnerabilities in SAP's Adaptive Servers

Description	
Cybersecurity researchers from Trustwave disclosed six different vulnerabilities in Sybase Adaptive Server Enterprise (ASE). The most severe vulnerability tracked CVE-2020-6248 allows arbitrary code execution when making database backups. Another vulnerability (CVE-2020-6252) is associated with ASE Cockpit which is a web-based administrative console. This allows attackers access to a local network to capture user account credentials, overwrite system files, execute malicious code with LocalSystem privileges in Windows system. Other vulnerabilities tracked CVE-2020-6241 and CVE-2020-6253 allows an authenticated user to execute crafted database queries to elevate their privileges via SQL injection which permits users with least privileges to gain database administrator access. CVE-2020-6243 allows Windows users to run arbitrary code and delete data on the ASE server when it does not perform necessary checks while authenticating users while executing a stored procedure ("dummy_esp"). Lastly CVE-2020-6250 allows authenticated users in Linux system to read system administrator passwords from installation logs. SAP has released security updates to patch these vulnerabilities.	
Source	https://thehackernews.com/2020/06/newly-patched-sap-ase-flaws-could-let.html
Infected Technology	Sybase Adaptive Servers
Recommendation	Update to the latest security patches
CVE	CVE-2020-6248, CVE-2020-6252, CVE-2020-6241, CVE-2020-6253, CVE-2020-6243, CVE-2020-6250

6. Fake Ransomware double encrypts victims' file

Description	
A tool advertised as decryption tool for STOP Djvu Ransomware is being actively distributed that instead is another ransomware which encrypts already encrypted file. The fake decryption tool, named Zorab, is falsely advertises to decrypt the files by Djvu Ransomware and once user starts the scan for decryption, extracts crab.exe file which encrypts the files in .ZRB extension and leaves a ransom note.	
Source	https://www.bleepingcomputer.com/news/security/fake-ransomware-decryptor-double-encrypts-desperate-victims-files/
Infected Technology	Windows
Recommendation	Do not install application from unknown source

7. VMware Cloud Director flaw lets hackers take over virtual datacenters

Description	
A code injection vulnerability in the VMware Cloud Director 10.0.0.2, 9.7.0.5, 9.5.0.6, and 9.1.0.4 that may lead to remote code execution. Cloud Director software allows cloud-service providers around the world to deploy, automate, and manage virtual infrastructure resources in a cloud environment. The severity of this vulnerability was evaluated by VMware as "important" with a CVSSV3 score of 8.8.	
Source	https://citadelo.com/en/blog/full-infrastructure-takeover-of-vmware-cloud-director-CVE-2020-3956/
CVE	CVE-2020-3956
Infected Technology	VMware Cloud Director
Recommendation	Update your VMware Cloud Director to the latest available version

8. O365 phishing baits remote workers with fake VPN config

Description	
Office 365 customers are being targeted by a phishing campaign that uses fake VPN update messages to steal login details. Security experts have flagged that the campaign looks to impersonate legitimate messages telling remote workers that they need to update their VPN configuration while working from home. The phishing emails used in the campaign are made to look as if they come from an organization's IT support department in an effort to lure employees into opening them. According to the email security firm, so far 15,000 targets have received these convincing phishing emails.	
Source	https://www.bleepingcomputer.com/news/security/office-365-phishing-baits-remote-workers-with-fake-vpn-configs/
Infected Technology	O365
Recommendation	Configure the block rules to O365

9. Proof-of-Concept available for Windows 10 SMBGhost with RCE exploit

Description	
Cybercriminals have been leveraging the vulnerability patched by Microsoft in March for affected windows 10 version 1909 and 1903 known as SMBGhost. They have been using it to escalate local privileges and deliver malware pieces such as the Ave Maria remote access trojan with keylogging and info stealing Capabilities.	
Source	https://www.bleepingcomputer.com/news/security/windows-10-smbghost-bug-gets-public-proof-of-concept-rce-exploit/
CVE	CVE-2020-0796
Infected Technology	Windows 10 [1909, 1903]
Recommendation	Patch your windows to the latest update

For any queries/recommendations:
Contact us: **whois@cryptogennepal.com**