November 23, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Facebook Messenger Bug
- Big Sur macOS Apps allowed to Bypass Firewall and VPNs
- VMware releases security updates
- Cisco fixed WebEx bugs allowing ghost participants in meetings
- Critical RCE flaw in Cisco Security Manager
- Drupal sites vulnerable to double extension attacks

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. Facebook Messenger Bug

Description

Facebook patched a bug on November 17, 2020 that allowed remote attackers to listen to the user before the user picked up the call. The bug was discovered on October 6th. It was reported by Google's Project Zero bug hunting team with a 90-day deadline. A message type which is not used for call set-up, SdpUpdate, causes setLocalDescription to be called immediately. If the message is sent to the user's device while it is ringing, it will start transmitting audio immediately, allowing the attacker to monitor the user's surroundings.

Source	https://bugs.chromium.org/p/project-zero/issues/detail?id=2098
Infected Technology	Facebook Messenger for Android version 284.0.0.16.119 and before
Recommendation	Update Messenger to the latest version

2. Big Sur macOS Apps allowed to Bypass Firewall and VPNs

Description

A new feature in the macOS Big Sur allows many of its apps to bypass firewalls and VPNs. Apple's NEFilterDataProvider allows monitoring of the Mac's network traffic by choosing to pass or block the data when receiving a new flow. By finding a way round the NEFilterFataProvider, it made it hard for the VPNs to block Apple applications. This leaves a gap allowing potential malwares to exploit and gain access to sensitive data.

Source	https://thehackernews.com/2020/11/apple-lets-some-of-its-big-sur-macos.html
Infected Technology	Apple macOS BIG SUR 11.0.1

3. VMware releases security updates

Description

VMware released fixes for vulnerabilities in VMware ESXi, Workstation, Fusion and Cloud Foundation. The vulnerabilities allowed code execution and privilege escalation. One of the bugs allowed attackers on a virtual machine with admin privileges to abuse a use-after-free vulnerability in the XHCI USB controller of the VMware ESXi, workstation and Fusion. The other bug allowed attackers to exploit a VMware ESXI privilege escalation bug in the way system calls are managed for escalating privileges.

Source	https://docs.vmware.com/en/VMware-vSphere/6.5/rn/esxi650-202011002.html
Infected Technology	VMware ESXi 6.5
CVE	CVE-2020-4004, CVE-2020-4005
Recommendation	Update to the patch release ESXi650-202011002

4. Cisco fixed WebEx bugs allowing ghost participants in meetings

Description

Cisco has fixed vulnerabilities WebEx Meeting that allowed unauthenticated remote attackers to join ongoing meetings as ghost participants. The flaw could be abused by threat actors to join meeting without being detected. The ghost users are participants that are not visible in user list, were not invited but can hear, speak and share media within the meeting. These users would also allow them to persist audio connection even after admin remove them from the meeting gaining access to user information such as email and IP address from meeting room lobby. The vulnerabilities exist in the handshake process that WebEx uses to establish a connection between meeting participants.

Source	https://securityintelligence.com/posts/ibm-works-with-cisco-exorcise-ghosts-webex-meetings/
Infected Technology	Cisco WebEx Meetings and Cisco WebEx Meetings Server
CVE	CVE-2020-3419, CVE-2020-3471, CVE-2020-3441
Recommendation	Update the patch released for on-prem solution

5. Critical RCE flaw in Cisco Security Manager

Description

Cisco has published multiple security advisories concerning critical flaws in Cisco Security Manager (CSM) a week after the networking equipment maker quietly released patches with version 4.22 of the platform. The 12 security vulnerabilities affecting the web interface of CSM that makes it possible for an unauthenticated attacker to achieve remote code execution (RCE) attacks. The vulnerabilities allow an attacker to craft malicious requests as well as upload and download arbitrary files in the context of the highest-privilege user account "NT AUTHORITYSYSTEM," giving the adversary access to all files in a specific directory.

Source	https://gist.github.com/Frycos/8bf5c125d720b3504b4f28a1126e509e
Infected Technology	Cisco Security Manager
Recommendation	Update the latest patch available by Cisco

6. Drupal sites vulnerable to double extension attacks

Description

Drupal, which is currently the fourth most used CMS on the internet after WordPress, Shopify, and Joomla, gave the vulnerability a rating of "*Critical*," advising site owners to patch as soon as possible. The team behind the Drupal content management system (CMS) has released this week security updates to patch a critical vulnerability that is easy to exploit and can grant attackers full control over vulnerable sites. Attackers can add a second extension to a malicious file, upload it on a Drupal site through open upload fields, and have the malicious executed.

Source	https://www.zdnet.com/article/drupal-sites-vulnerable-to-double-extension-attacks/?&web_view=true
Infected Technology	Drupal site
CVE_ID	CVE-2020-13671

For any queries/recommendations:

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