November 09, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- VMware Issues updated fix for critical ESXi flaw
- 0-day in Cisco AnyConnect Secure Mobility Client yet to be fixed
- Multiple vulnerabilities in Adobe Acrobat reader
- Sangoma PBX exploited by attackers to abuse SIP servers
- NAT Slipstreaming
- Critical bug actively used to deploy Cobalt Strike on Oracle Server
- Apple patches three actively exploited iOS zero-days

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 Issues updated fix for critical ESXi flaw

Description
VMware has released an updated fix for a critical remote code execution flaw affecting ESXi product mentioning previous fix was incomplete. The previous patch which was released on October 20 did not cover certain version. The flaw exists in the OpenSLP feature of VMware ESXi which allows systems to discover services available in network for use. The flaw has a score of 9.8 out of 10 which result in remote code execution with improper implementation of free after use memory location.

Source	https://www.vmware.com/security/advisories/VMSA-2020-0023.html
Infected Technology	VMware ESXi version 7, 6.7 and 6.5
CVE_ID	CVE-2020-3992
Recommendation	Update to the newer version

2. 0-day in Cisco AnyConnect Secure Mobility Client yet to be fixed

Description
Cisco has disclosed a 0-day vulnerability in Cisco AnyConnect Secure Mobility Client software with public availability of proof-of-concept exploit code. The flaw resides in interprocess communication (IPC) channel of Cisco AnyConnect Client which can be exploited by authenticated local attacker to execute malicious scripts via targeted user. This allows attacker to execute a script with privilege of targeted user. The vulnerability affects Windows, Linux and macOS while iOS and Android are not impacted. The targeted user must be in active session. Cisco has not yet released the fix but is expected to include in future AnyConnect client release.

Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-ipc-KfQO9QhK
Infected Technology	Cisco AnyConnect Secure Mobility Client for Windows, Linux and MacOS
CVE	CVE-2020-3556
Recommendation	Disable Auto Update feature Update the version once fixed version is released

3. Multiple vulnerabilities in Adobe Acrobat reader

Description	
Researchers at Cisco Talos has discovered a heap buffer overflow vulnerability in Adobe Acrobat Reader. A specially crafted malicious file of web page can trigger the vulnerability which can lead to sensitive information leading to arbitrary code execution. The vulnerability was patched on fifth of April however is present in the new version. Similarly, a specific JavaScript code embedded in a PDF file can lead a heap corruption leading to code execution. A patch to fix the vulnerability has been released.	
Source	https://blog.talosintelligence.com/2020/11/vulnerability-spotlight-multiple.html?&web_view=true
Infected Technology	Adobe Acrobat Reader
CVE	CVE-2020-24435, CVE-2020-24437
Recommendation	Update the patches released

4. Sangoma PBX exploited by attackers to abuse SIP servers

Description	
Researchers from Check Point have released a finding mentioning threat vectors have targeted Sangoma PBX, an open-sourced user interface that's used to control Asterisk VoIP phone systems particularly SIP servers. This allowed attacker to make any outgoing calls, sell phone numbers, call plans and live access to highest bidders. The attackers exploited a year-old vulnerability impacting administrative web interface of FreePBX and PBXact.	
Source	https://blog.checkpoint.com/2020/11/05/whos-calling-gaza-and-west-bank-hackers-exploit-and-monetize-corporate-voip-phone-system-vulnerability-internationally/
Infected Technology	Sangoma PBX
CVE	CVE-2019-19006
Recommendation	Apply patch for mentioned vulnerability Create strong password policy and audit servers for any backdoor uploads

5. NAT Slipstreaming

Description
Security Researcher has discovered a technique that allows an attacker to bypass NAT/Firewall protections, leading to remote access of any TCP/UDP port service on the target system. NAT Slipstreaming is attack involves social engineering, the attacker sends the victim a link to malicious site or a legitimate site adware. When they visit the site, the attacker can open any TCP or UDP port on the victim's system, bypassing client-side port restrictions. It is important that this is an attack which demonstrates the impact of social engineering, it doesn't matter if the Firewall is configured properly, this attack relies on deception rather than a misconfiguration or vulnerability.

Source	https://samy.pl/slipstream/
Infected Technology	NAT Application Level Gateway
Recommendation	Raising Awareness program of Social engineering attacks

6. Critical bug actively used to deploy Cobalt Strike on Oracle Server

Description
Attacker actively exploiting Oracle WebLogic servers to deploy Cobalt Strike beacons which allow for persistent remote access to compromised devices. Cobalt Strike is a legitimate penetration testing tool also used by threat actors in post-exploitation tasks and to deploy so-called beacons that enable them to gain persistent remote access. It allows them to access the compromised servers to harvest data and to deploy second stage malware payloads.

Source	https://attack.mitre.org/software/S0154/
Infected Technology	Oracle Server
CVE	CVE-2020-14882, CVE-2020-14750
Recommendation	Apply the security updates to block attacks

7. Apple patches three actively exploited iOS zero-days

Description	
Apple has patched today three iOS zero-day vulnerabilities actively exploited in the wild and affecting iPhone, iPad, and iPod devices. The attacks were discovered by Google's Project Zero vulnerability research group, which over the past few weeks has detected four other zero-day exploits—three against Chrome and a third against Windows. The flaws are CVE-2020-27930 a code-execution vulnerability that attackers can trigger using maliciously crafted fonts ,CVE-2020-27950, which allows a malicious app to obtain the locations in kernel memory, and CVE-2020-27932, a bug that allows code to run with highly privileged system rights.	
Source	https://support.apple.com/en-us/HT211929
Infected Technology	• iPhone 6s and later • iPod touch 7th generation • iPad Air 2 and later • iPad mini 4 and later
Recommendation	Update the patch released of iOS 14.2
CVE	CVE-2020-27930, CVE-2020-27950, CVE-2020-27932

For any queries/recommendations:

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