October 12, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Cisco warns to patch Webex Teams for Windows and surveillance camera
- Linux kernel vulnerable to local privilege escalation
- HashiCorp Vault Vulnerabilities leads to authentication Bypass
- Cyber Criminals Abuses Built-in Services to Target Windows
- Cyber Criminals using ZeroLogon to spread ransomware
- Multiple Vulnerabilities on QNAP Help desk app

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. Cisco warns to patch Webex Teams for Windows and surveillance camera

Description

Cisco has released a patch update for high severity security flaws for Webex Teams for Windows, Cisco's Identity service Engine and 8000 Series IP cameras. 8000 Series IP Camera is the most affected with Remote Code Execution (RCE) and Denial of Service (DoS) with severity of 8.8 out of 10. The vulnerability does not affect products updated to firmware release 1.0.9-4 and later. Another vulnerability is due to unenforced Role-based access control in Web management interface of Cisco Identity Services with score of 7.7. A remote attacker with read-only credential could modify vulnerable device's configuration using crafted HTTP request. Another flaw affecting Cisco's Webex Teams client for windows allows local attacker with system access to load malicious DLL file that execute when Webex Teams is launched. Cisco has also released security advisory for various products with Medium severity vulnerabilities including Privilege escalation, path traversal and 9 other flaws.

Source	https://tools.cisco.com/security/center/publicationListing.x
Infected Technology	Cisco Webex Teams for Windows (3.0.13464 - 3.0.16040.0) Cisco ISE 2.3, 2.4, 2.5, 2.6 and 2.7 Cisco Video Surveillance 8000 Series IP Camera <=1.0.9-5
CVE	CVE-2020-3535, CVE-2020-3467, CVE-2020-3544
Recommendation	Update the patch released

2. Linux kernel vulnerable to local privilege escalation

Description

Researcher from Palo Alto has identified a memory corruption vulnerability in Linux kernel. The identify vulnerability can used to perform privilege escalation in Linux system. The vulnerability requires *AF_PACKET* sockets enabled and *CAP_NET_RAW* privilege for triggering the process. Both of which are enabled by default in distributions like Ubuntu. The vulnerability has not been patched however, use of various security products available can be a workaround the vulnerabilities.

Source	https://unit42.paloaltonetworks.com/cve-2020-14386/
Infected Technology	Linux kernel
CVE	CVE-2020-14386
Recommendation	Use Privilege Escalation protection tools

3. HashiCorp Vault Vulnerabilities leads to authentication Bypass

Description

HashiCorp Vault is a widely used cloud-native software that can store, generate, and access secrets such as API keys, credentials, and certificates. The technology can provide temporary credentials to services or third-party resources such as an AWS S3 bucket. HashiCorp Vault can be configured with popular resources including AWS and GCP. The two vulnerabilities in Vault could allow an attacker to bypass authentication checks in AWS and GCP. First one enables an attacker to bypass authentication within Vault server for configuration with AWS whereas second one is complex logic bug in the authentication Process for deployment on Google cloud.

Source	https://googleprojectzero.blogspot.com/2020/10/enter-the-vault-auth-issues-hashicorp-vault.html
Infected Technology	Amazon Web Services (AWS), Google Cloud Platform
Recommendation	Update the patch released by respective vendors.

4. Cyber Criminals Abuses Built-in Services to Target Windows

Description

Cybercriminals are now abusing inbuilt legitimate services of windows to perform fileless attacks. Researchers disclosed, spear-phishing emails are used to spread a zip file containing a malicious document. A new attack dubbed kraken was identified abusing Windows Error Reporting (WER) service as an evasion mechanism.The attackers target Windows internal service WerFault[.]exe, which is used to report an error that occurs in the Windows OS. They first compromise a website to host their payload and use the CactusTorch framework to execute a fileless attack accompanied by multiple tricks. After passing the anti-analysis checks, it loads the final shellcode and creates a new WER thread.

Source	https://cyware.com/news/cybercriminals-abuse-built-in-services-to-target-windows-1ac08ad2
Infected Areas	Windows
Recommendation	User must regularly update anti-virus solutions, update Windows, and deploy a malicious behavior monitoring mechanism.

5. Cyber Criminals using ZeroLogon to spread ransomware

Description

Microsoft is warning that cybercriminals have started to incorporate exploit code for the ZeroLogon vulnerability in their attacks. The alert comes after the company noticed ongoing attacks from cyber-espionage group MuddyWater (SeedWorm) in the second half of September. TA505 has been delivering a wide variety of malware, from backdoors to ransomware. Recently, intrusions from this group are followed by the deployment of Clop ransomware, as in the attack on Maastricht University last year that resulted in paying a 30 bitcoin (about $220,000) ransom.

Source	https://www.bleepingcomputer.com/news/security/ransomware-gang-now-using-critical-windows-flaw-in-attacks/
Infected Technology	Windows OS
CVE	CVE-2020-1472
Recommendation	Update your system to the latest Windows version.

6. Multiple Vulnerabilities on QNAP Help desk app

Description

Two new vulnerabilities on QNAP's helpdesk app could have led potential attackers to take over unpatched QNAP NAS. Helpdesk is the built-in app that comes with QNAP's NAS devices and allows admins to submit help requests to the QNAP support team over the Internet. The app also comes with a remote support feature that allows remotely connecting to the device with the owner's permission.

Source	https://www.qnap.com/en/security-advisory/QSA-20-08
Infected Technology	QNAP Help desk app
CVE	CVE-2020-2506 and CVE-2020-2507
Recommendation	To fix the vulnerability, we strongly recommend updating Helpdesk to the latest version.

For any queries/recommendations:

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