October 5, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Cisco released patches for high severity Flaws
- HP device manager backdoor resulting in windows System Takeover
- Windows Subsytem for Linux 2 bypasses Windows Firewall
- Critical Flaws in popular Industrial Remote Access System
- Emotet malware takes part in the 2020 U.S. elections
- Remote Code Execution Bugs in NVIDIA D3D10

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 released patches for high severity flaws.

Description	
Cisco has released patches for three high severity flaws on Tuesday. Two of the flaws result in DoS which are present is Cisco's carrier grade and data center routers. Both vulnerabilities are present in Cisco IOS Software's Distance Vector Multicast Routing Protocol (DVMRP) and affect all Cisco devices configured with Multicast routing and receiving DVMRP traffic. The vulnerability allows remote unauthenticated attacker to send specially crafted IGMP packet resulting in crash IGMP process. Another high severity vulnerability allows local authenticated user to execute persistent code at boot time and break chain of trust. The code execution flaw is due to incorrect validation of ROM monitor (ROMMON) variable. The exploitation of this vulnerability required access to root shell on device or physical access.	
Source	https://tools.cisco.com/security/center/publicationListing.x
Infected Technology	Cisco
CVE	CVE-2020-3451, CVE-2020-3453, CVE-2020-3417
Recommendation	Apply the update released by the OEM

2. HP device manager backdoor resulting in Windows System takeover

Description	
HP has released security advisory of three critical and high severity vulnerability in HP Device manager that leads to system takeover. HP Device Manger is used to manage thin clients. The flaws in Device Manager include weak cipher implementation, remote method invocation and privilege escalation to system access. HP has released security update for privilege escalation and partial mitigation step for other two vulnerabilities. The two unpatched vulnerabilities effect all HP Device Manager version with the score of 7.0 and 9.9 respectively.	
Source	https://support.hp.com/us-en/document/co6921908
Infected Technology	HP Device Manager
CVE	CVE-2020-6925, CVE-2020-6926, CVE-2020-6927
Recommendation	• Use the current version of HP Device Manager (v 5.0.4) • Apply the remediation steps listed in the advisory for unpatched vulnerabilities for partial mitigation

3. Windows Subsytem for Linux 2 bypasses Windows Firewall

Description	
The Windows Subsystem for Linux 2 will bypass any Windows 10 firewall rules. The vulnerability was posted in a blog by Mullvad VPN. The vulnerability exists since the introduction of WSL 2. WSL 2 uses a true Linux kernel operating in Hyper-V virtual machine with Hyper-V virtual network adapter. When using WSL2 the network connection bypasses the firewall rule to 'Always require VPN'.	
Source	https://mullvad.net/en/blog/2020/9/30/linux-under-wsl2-can-be-leaking/
Infected Technology	Windows Subsytem for Linux (WSL) 2

4. Critical Flaws in Popular Industrial Remote Access Systems

Description	
Researchers at an Israeli operational Technology (OT) Company have discovered multiple critical vulnerabilities in two popular industrial remote access software solutions. The Flaws can be exploited to access industrial production floors, break into company networks, tamper with data, or steal highly sensitive trade secrets. Researchers discovered the vulnerabilities in remote access systems made by Austrian automation and process control technology company. Researcher noted that by exploiting the B&R flaws, an attacker who has gained authorized access to the B&R solution can view sensitive information about other users whose information resides on the same server. the vulnerability found in a highly accessible zone of mbConnect24 allowed an attacker to leverage a vulnerable, outdated library to upload crafted authentication files.	
Source	https://www.otorio.com/news-events/press-release/otorio-discovers-critical-vulnerabilities-in-leading-industrial-remote-access-software-solutions/
Infected Areas	**B&R automations** • Sitemanager prior to v9.2.620236042 • GateManager 4260 and 9250 before v9.0.20262 • GateManager 8250 prior to v9.2.620236042 **mbConnect Line**
Recommendation	Update the latest patch available

5. Emotet malware takes part in the 2020 U.S. elections

Description
Hundreds of U.S. organizations were targeted by an Emotet spear-phishing campaign, which sent thousands of emails purporting to be from the Democratic National Committee and recruiting potential Democratic volunteers. When the Emotet gang sends out spam, their main goal is to convince recipients to open the attached malicious document. This is usually done through email themes that pretend to be shipping documents, invoices, payment receipts, and voicemails. During the holidays or major political events, Emotet is known to send more themed emails to convince users to open attachments. Once the attachments are opened, and macros enabled, the Emotet malware will be installed on a computer. It will then steal your emails and use your computer to send out further spam.

Source	https://www.proofpoint.com/us/blog/threat-insight/emotet-makes-timely-adoption-political-and-elections-lures
Infected Areas	U.S. Election
Recommendation	Do not click link or open attachment from unknown sender

6. Remote code Execution bugs in NVIDIA D3D10 Driver

Description
NVDIA Graphics drivers is software for NVIDIA Graphics GPU installed on the PC. It is used to communicate between the operating systems and GPU device. Cisco Talos discovered multiple remote code execution vulnerabilities in the NVDIA D3D10 driver. This driver supports multiple GPUs that NVIDIA produces. An adversary could exploit these vulnerabilities by applying the user with a malformed shader, eventually allowing them to execute code on the victim machine. This vulnerability can be triggered by supplying a malformed pixel shader. This leads to a memory corruption problem in the NVIDIA driver.

Source	https://emvrace.github.io/
Infected Technology	NVIDIA D3D10 Driver version 422.50-26.21.14.425-
CVE_ID	CVE-2020-5981

For any queries/recommendations:

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