August 23, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- ProxyShell exploitation found on Microsoft Exchange servers
- Chinese Espionage Groups discovered using ShadowPad
- Critical bug in Cisco's Small business routers to remain unpatched
- Evidence of Diavol Ransomware linked to TrickBot Gang
- Windows EoP Bug Detailed by Google Project Zero
- Server Name Identification Vulnerability affects multiple Cisco Products

CryptoGen Nepal

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.

ProxyShell exploitation found on Microsoft Exchange servers

Description	
On-going active exploitation attempts have been discovered by the U.S. Cybersecurity and Infrastructure Security Agency that leverage the latest line of "ProxyShell" Microsoft Exchange vulnerabilities that were patched in the month of May. The vulnerabily is known to bypass ACL control, elevate privileges on the Exchange PowerShell backedn, effectively permitting the attacker to perform unauthenticated, RCE (Remote Code Execution). The attackers are seen to be installing web shells as a backdoor on the vulnerable servers.	
Source	https://therecord.media/almost-2000-exchange-servers-hacked-using-proxyshell-exploit/
Infected Technology	Exchange Server
Recommendation	Monitor for exploitation attempts and apply all available patches
CVE-ID	CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207

Chinese Espionage Groups discovered using ShadowPad

Description	
The successor to PlugX, chinese threat actors are currently utilizing a privately sold malware known as ShadowPad. Cyber Security organization SentinelOne has identified at least five threat actor groups known to use this malware, which includes, APT41, Tick & Tonto Team, Operation Redbounis, operation RedKanku, and Fishmonger. The malware is known to use backdoors which gives persistence access to the threat actors and execute malicious commands. The malware are seen to propagate through Trojanized software installers.	
Source	https://labs.sentinelone.com/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/
Infected Technology	Vulnerable Server Management software
Recommendation	Keep anti-malware solution and operating systems up to date

Critical bug in Cisco's Small business routers to remain unpatched

Description	
A critical security vulnerability in Cisco Small Business Routers allows remote code execution and denial of service are said to be remain unpatched as cisco will not be providing patches for these devices. Cisco claims the reason for this is because the routers had reached end-of-life back in 2019. The vulnerability currently residing in the devices have CVSS score of 9.8 out of 10. The cause of this vulnerability is due to improper validation of incoming UPnP traffic.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-sb-rv-overflow-htpymMB5
Infected Technology	Cisco RV110W, RV130, RV130W and RV215W models
Recommendation	Replace EOL (End of Life) devices
CVE-ID	CVE-2021-34730

Evidence of Diavol Ransomware linked to TrickBot Gang

Description	
The details about an early development version of a nascent ransomware, Diavol being linked with the perpetrators behind the TrickBot syndicate has surfaced. Latest findings from IBM X-Force show similarities to malwares from the cybercrime gang. An early sample of Diavol which was compiled on March 5, 2020 and submitted to Virus Total on January 27, 2021 showed the process of the malware development consisting of source code capable of terminating random processes and prioritizing file types to encrypt based on a pre-configured list of extensions readied by the attacker.	
Source	https://securityintelligence.com/posts/analysis-of-diavol-ransomware-link-trickbot-gang/
Infected Technology	SAP Products
Recommendation	Apply all Patches and updates

Windows EoP Bug Detailed by Google Project Zero

Description	
A couple of months ago, Google disclosed a Windows bug that could cause elevation of privilege (EoP) following a botched fix from Microsoft, and today, it has done almost exactly the same. he gist of the matter is that the default rules of the Windows Filtering Platform (WFP) permit executable files to connect to TCP sockets in AppContainers, which leads to EoP. Essentially, some rules defined in WFP can be matched by a malicious actor to connect to an AppContainer and inject malicious code.	
Source	https://bugs.chromium.org/p/project-zero/issues/detail?id=2207&can=2&q=&colspec=ID%20Type%20Status%20Priority%20Milestone%20Owner%20Summary&cells=ids
Infected Technology	Windows 10 2004, 21H1

Server Name Identification Vulnerability affects multiple Cisco Products

Description	
Cisco has released a security advisory stating a vulnerability that allows attacker to bypass TLS inspection filtering in multiple products to exfiltrate data. The vulnerability resides in Server Name Identification (SNI) request filtering impacts 3000 Series Industrial Security Appliances (ISAs), Firepower Threat Defense (FTD) and Web Security Appliance (WSA) products. Attacker can exfiltrate data in SSL hello packet because hello packet response from server on blocked list is not filtered which can be used to execute C2C attack.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sni-data-exfil-mFgzXqLN
Infected Technology	Cisco products: 3000 Series ISAs FTD Software WSA

Recommendation	Apply the fix once released by OEM

For any queries/recommendations:

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

OUR SERVICES

Our services as information security company includes:


INFORMATION SECURITY AUDIT


VULNERABILITY ASSESSMENT


PENETRATION TESTING


MANAGED/CO.MANAGED SOC


INCIDENT RESPONSE


THREAT ANALYSIS


SERVER HARDENING


CYBER SECURITY CONSULTANT


INFORMATION SECURITY TRAINING

CryptoGen Nepal

https://www.facebook.com/CryptoGenNepal/
https://twitter.com/CryptoGenNepal
https://www.instagram.com/CryptoGenNepal/