July 05, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- All versions of Windows affected with PrintNightmare
- Cisco ASA vulnerability actively exploited after exploit released
- NETGEAR Routers vulnerable to three new vulnerabilities
- Widespread Brute force attack tied to APT28 using Kubernetes Cluster
- Linux variant of REvil Ransomware targeting ESXi and NAS Devices

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.

1. All versions of Windows affected with PrintNightmare

Description	
A new vulnerability has been identified in all version of Windows which allows an attacker to run arbitrary code with SYSTEM privilege in affected device. The vulnerability exists in the Windows Printer Spooler service. All Windows version are vulnerable to the vulnerability via Windows Printer Spooler service on domain controller. Microsoft has suggested users to disable the service until the service has been patched.	
Source	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
Infected Technology	Windows
CVE-ID	CVE-2021-34527
Recommendation	Disable the Windows Printer Spooler Service Apply the patch once available

2. Cisco ASA vulnerability actively exploited after exploit released

Description	
A security vulnerability in Cisco Adaptive Security Appliance (ASA) is cross-site scripting that was patched by the Cisco last October and again early this April has been exposed to active in-the-wild attacks as a result of the availability of proof-of-concept (PoC) exploit code. Multiple vulnerabilities in the web services interface of Cisco ASA software and Cisco Firepower Threat Defense (FTD) software could allow an unauthenticated, remote attacker to execute cross-site scripting (XSS) attacks on an affected device.	
Source	https://twitter.com/ptswarm/status/1408050644460650502
Infected Technology	Cisco ASA
CVE-ID	CVE-2020-3580
Recommendation	Apply the latest patch available.

3. NETGEAR Routers vulnerable to three new vulnerabilities

Description	
Microsoft has identified some critical firmware vulnerability in some NETGEAR router of DGN2200v1 series. The vulnerability allows an unauthenticated attacker to access router management page, bypass authentication and gain secret stored on the device. NETGEAR has addressed the issue and released new firmware update to path the vulnerable devices.	
Source	https://kb.netgear.com/000062646/Security-Advisory-for-Multiple-HTTPd-Authentication-Vulnerabilities-on-DGN2200v1
Infected Technology	NETGEAR DGN2200v1 series router
Recommendation	Update the firmware for affected devices

4. Widespread Brute force attack tied to APT28 using Kubernetes Cluster

Description	
A joint research by NSA, CISA, FBI and UK's NCSC has identified a mass brute force and password spraying attack targeting cloud services such as O365. The attack has been APT28 group and has been on going since late 2019. The APT group is known to use the previously disclosed vulnerability in Microsoft Exchange Server and has recently seen to use Kubernetes cluster along with Tor network with VPN services for anonymity. The research suggests disabling Tor services and enforce the use of MFA across network.	
Source	https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF
Recommendation	Disable Tor and VPN(external) services whereable possible Enforce use of MFA across devices and services.

5. Linux variant of REvil Ransomware targeting ESXi and NAS Devices	
Description	
Attackers behind REvil ransomware has ported the malware to Linux to target VMware's ESXi and NAS devices. Researches at AT&T Cybersecurity has confirmed four sample of these ported malwares. The malware can affect *nix systems and ESXi and share the similar attribute to Windows variant of the ransomware and use encryption extensions as .rhkrc, .qoxaq, .naixq, and . 7rspj.	
Source	https://cybersecurity.att.com/blogs/labs-research/revils-new-linux-version
Infected Technology	VMware ESXi, NAS Devices

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/