September 13, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Google Android Security Update Patches 40 Vulnerabilities
- Microsoft Azure Account Takeover
- PoC released Authentication Bypass Bug in NETGEAR Switches
- Microsoft MSHTML RCE vulnerability actively exploited
- High-Severity Flaws in IOS XR parched by CISCO

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.

Google Android Security Update Patches 40 Vulnerabilities	
Description	
Google has issued the latest Android Security Bulletin, which addresses a total of 40 vulnerabilities. Patches for seven major vulnerabilities were included in the monthly release. The most serious flaw fixed was a major vulnerability in the Framework component. According to the warning, the flaw may let a remote attacker to create a persistent denial of service by using a carefully designed failure. Six additional vulnerabilities in the Framework component were fixed, all of which were rated as critical.	
Source	https://source.android.com/security/bulletin/2021-09-01
Infected Technology	Android 8.1,9,10, and 11
Recommendation	Update the patch available
CVE_ID	CVE-2021-0687

Microsoft Azure Account Takeover	
Description	
Microsoft announced that it had fixed a vulnerability in its Azure Container Instances (ACI) services that could have been exploited by a malicious actor "to access other customers' information," in what the researchers called the "first cross-account container takeover in the public cloud." An attacker who takes advantage of the flaw might execute arbitrary instructions on the containers of other users, steal customer secrets and images deployed to the platform	
Source	https://www.cyberark.com/resources/threat-research-blog/blackdirect-microsoft-azure-account-takeover
Infected Technology	Microsoft azure
Recommendation	Update the latest available patch
CVE_ID	CVE-2019-5736

PoC released Authentication Bypass Bug in NETGEAR Switches

Description	
Netgear has released patches to address three security vulnerability affecting smart switches. The flaw when abused can be used by threat vectors to gain full control of vulnerable device. The vulnerabilities are an authentication bypass, an authentication hijacking, and an undisclosed vulnerability. The vulnerability has been provided with CVSS score 9.8 and 7.8.	
Source	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145
Infected Technology	Multiple NETGEAR Devices
Recommendation	Update the firmware released by OEM
CVE-ID	N/A

Microsoft MSHTML RCE vulnerability actively exploited

Description	
Microsoft has disclosed a vulnerability affecting MSHTML, also known as Trident, which is actively being exploited. The vulnerability is a remote code execution which is being attacked in wild using specially crafted malicious Microsoft Office Documents. MSHTML is a legacy proprietary browser engine used in Internet Explorer.	
Source	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
Infected Technology	Microsoft Windows
Recommendation	Disable ActiveX controls in Microsoft Internet Explorer
CVE-2021-40444	CVE-2021-40444

High-Severity Flaws in IOS XR parched by CISCO

Description	
CISCO has patched a high-severity vulnerability in the IOS XR software. The vulnerabilities could be exploited for privilege escalations, rebooting devices, overwriting, and read arbitrary files.	
Source	https://tools.cisco.com/security/center/viewErp.x?alertId=ERP-74637
Infected Technology	ASR 9000 series, IOS XR
Recommendation	Apply patches provided
CVE-ID	CVE-2021-34720, (CVSS score 8.6) CVE-2021-34718, (CVSS 8.1) CVE-2021-34719, CVE-2021-34728 CVE-2021-34713

Zoho patches critical ADSelfService Plus bug

Description	
ADSelfService Plus, an integrated self-service password management and a single sign-on solution for Active Directory and cloud apps had some of its security issues identified. The vulnerabilities allow perpetrators to bypass admin portal access-restriction, CAPTCHA bypass and remote code executions.	
Source	https://www.bleepingcomputer.com/news/security/zoho-patches-actively-exploited-critical-adselfservice-plus-bug/?&web_view=true
Infected Technology	Zoho’s ManageEngine ADSelfService
Recommendation	Apply the latest updates from the developer trough the service pack.
CVE-ID	CVE-2021-40539 CVE-2021-37421 CVE-2021-37417 CVE-2021-33055 CVE-2021-28958

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/