December 6, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- HP Printer vulnerable to wormable security flaw
- 0patch releases patches for Windows 10 zero day
- Use-after-free condition in Google Chrome could lead to code execution
- Project Zero Flags High-Risk Zoom Security Flaw
- Critical Bug in Mozilla's NSS Crypto Library Potentially Affects Several Other Software

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.

HP Printer vulnerable to wormable security flaw

Description	
Cybersecurity researchers from F-Secure Labs have disclosed eight-year-old security flaw that affects 150 different multifunctional printers from HPs. The vulnerability can be exploited to take control over vulnerable device. The disclosed vulnerabilities have severity rating of 9.3 and 7.1 respectively. The vulnerability is wormable allowing exploit to propagate to other infected devices in the network.	
Source	https://labs.f-secure.com/publications/printing-shellz
Infected Technology	HP multi-function printers
Recommendation	• Limit physical access to the printing devices • Enforce network segmentation

opatch releases patches for Windows 10 zero day

Description	
0patch has released free unofficial patches for Windows local privilege escalation zero-day. The flaw is present in Mobile Device Management Service discovered by security researched Abdelhamid Naceri. The flaw impacts windows 10 with system protection enabled in C drive. 0patch has provided with temporary unofficial patches for the flaw until official patch has been provided by Microsoft	
Source	https://securityaffairs.co/wordpress/125061/security/unofficial-patches-cve-2021-24084-zeroday.html?web_view=true
Infected Technology	Windows 10 v1809 and later
Recommendation	Apply the official patch once released by OEM
CVE_ID	CVE-2021-24084

Use-after-free condition in Google Chrome could lead to code execution

Description	
Google Chrome is a cross-platform web browser — and Chromium is the open-source version of the browser that other software developers use to build their browsers, as well. This specific vulnerability exists in Blink, the main DOM parsing and rendering engine at the core of Chromium. Cisco Talos recently discovered an exploitable use-after-free vulnerability in Google Chrome. is a use-after-free vulnerability that triggers if the user opens a specially crafted web page in Chrome. That page could trigger the reuse of previously freed memory, which can lead to arbitrary code execution.	
Source	https://blog.talosintelligence.com/2021/12/vuln-spotlight-chrome-.html?&web_view=true
Recommendation	Update the latest available patch.
CVE_ID	CVE-2021-30625

Project Zero Flags High-Risk Zoom Security Flaw

Description	
Zoom video conferencing software host sent security crash episodes exposing users of Windows, MacOS, Linux, iOS and Android to malicious criminals. he flaws, discovered and reported by Google Project Zero researcher, affect the company's flagship Zoom Client for Meetings on all major platforms and could be exploited for code execution attacks. This can potentially allow a malicious actor to crash the service or application, or leverage this vulnerability to execute arbitrary code	
Source	https://www.securityweek.com/project-zero-flags-high-risk-zoom-security-flaw?&web_view=true
Infected Technology	Zoom
Recommendation	Update the latest available patch.
CVE_ID	CVE-2021-34423, CVE-2021-34424

Critical Bug in Mozilla's NSS Crypto Library Potentially Affects Several Other Software

Description	
A new critical security weakness has been disclosed by Mozilla and provided fixes to address the vulnerability that could be potentially exploited by an adversary to crash a vulnerable application and even execute arbitrary code. The vulnerability resides in a cross-platform Network Security Service which is a collection of open-source cryptographic computer libraries designed to enable cross-platform development of client-server applications.	
Source	https://www.mozilla.org/en-US/security/advisories/mfsa2021-51/
Infected Technology	NSS versions prior to 3.73 or 3.68.1 ESR
Recommendation	Update your NSS with latest patch release.
CVE_ID	• CVE-2021-43527

ManageEngine ServiceDesk plus vulnerability exploited

Description	
A critical vulnerability in the Zoho ManageEngine ServiceDesk Plus is being exploited by an APT group. Attackers can upload executable files and place webshells that enable them to conduct post-exploitation activities as compromising admin credentials, lateral movement, exfiltrating registry hives and AD files following a successful exploitation of the vulnerability.	
Source	https://www.helpnetsecurity.com/2021/12/03/cve-2021-44077/?web_view=true
Infected Technology	Zoho ManageEngine ServiceDesk Plus v11305 and earlier
Recommendation	Update to Zoho ManageEngine ServiceDesk Plus build 11306, or higher Review Zoho security advisory for further remediation guide
CVE-ID	CVE-2021-44077

Hidden Payment data Stealing Malware in Nginx Process

Description	
A number of E-commerce platforms based on U.S, France and Germany have fallen victim to a new form of malware. The code injects itself into host Nginx application and masquerades its presence. Also known as NginRAT, the threat was found on eCommerce servers that had been infected with CronRat a remote access trojan (RAT) that hides payloads in tasks scheduled to execute on an invalid day of the calendar. CronRAT and NginRAT provide a remote connection to the compromised servers, they then make server-side modifications to the compromised e-commerce websites in a manner that enable the adversaries to exfiltrate data by skimming online payment forms.	
Source	https://thehackernews.com/2021/12/new-payment-data-sealing-malware-hides.html?&web_view=true
Infected Technology	Nginx Server

Fake Adobe Windows App Installer Packages Distributing Emotet Malware

Description	
Emotet malware, also known as a banking trojan is now being distributed via malicious Windows App Installer packages that masquerade as Adobe PDF applications. The threat actors behind Emotet are now infecting PCs by installing malicious packages using App Installer which is a built-in function of Windows 10 and Windows 11. Once the installation is approved by prospect victims following a link and prompt for a PDF document, the link launches an app installer which downloads and installs the malicious appxbundle hosted on Microsoft Azure. This appxbundle will place a DLL in the %Temp% folder and launch it using rundll32.exe.	
Source	https://blog.malwarebytes.com/ransomware/2021/12/emotet-being-spread-via-malicious-windows-app-installer-packages/?web_view=true https://www.malwarebytes.com/emotet
Infected Technology	Windows App installer packages
Recommendation	Avoid approving the installation of “Adobe PDF Component”

Apache HTTP server vulnerability Exploited

Description	
News of a recently patched Apache HTTP Server being exploited in attack has surfaced. The vulnerability is a server-side request forgery (SSRF) which can be exploited against httpd web servers that have the mod-proxy module enabled. Attackers can leverage this critical flaw using a specially crafted request to cause the mod-proxy module to route the connections to an selected origin server to exfiltrate sensitive data.	
Source	https://www.helpnetsecurity.com/2021/12/03/cve-2021-44077/?web_view=true
Infected Technology	Apache HTTP Server till v2.4.48
Recommendation	Upgrade to Apache HTTP Server 2.4.49 and later
CVE-ID	CVE-2021-40438

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/