September 6, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- **WooCommerce Pricing Plugin Allows Malicious Code-Injection**
- **Vendors Issue Security Advisories for OpenSSL Flaws**
- **Cisco fixes critical flaw in Enterprise NFVIS**
- **Popular TP-Link router ships with vulnerable firmware**
- **AMD chips are vulnerable to Meltdown-like attack**

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.

WooCommerce Pricing Plugin Allows Malicious Code-Injection	
Description	
Unauthorized attackers may be able to run arbitrary harmful scripts into unencrypted websites due to security vulnerabilities in Envato's WooCommerce Dynamic Pricing and Discounts plugin. This can result in a variety of attacks, including website redirections to phishing pages and the injection of malicious code on product pages. The two unauthenticated vulnerabilities affect version 2.4.1 and below, is a high-severity stored cross-site scripting (XSS) bug; the second is a medium-severity settings export problem.	
Source	https://blog.nintechnet.com/woocommerce-dynamic-pricing-and-discounts-plugin-fixed-multiple-vulnerabilities
Infected Technology	WooCommerce Platform
Recommendation	Update immediately if you have 2.4.1 or below installed.

Vendors Issue Security Advisories for OpenSSL Flaws	
Description	
Several companies that use the OpenSSL cryptography library toolkit are reportedly scrambling to release security advisories to their users following patching of two vulnerabilities in the library, which were first fixed and disclosed to users. The companies are now informing users about the affected products, versions, and fixes available for these flaws. a high-severity, critical SM2 decryption buffer overflow vulnerability, and another high-severity, buffer overrun flaw that can result in a denial-of-service attack.	
Source	https://www.securityweek.com/companies-release-security-advisories-response-new-openssl-vulnerabilities?&web_view=true
Infected Technology	OpenSSL
Recommendation	Update the latest available patch
CVE_ID	CVE-2021-3711, CVE-2021-3712

Cisco fixes critical flaw in Enterprise NFVIS

Description	
Cisco has released patches for critical authentication bypass vulnerability in NFV Infrastructure software. The PoC exploit code for the vulnerability was publicly available. When exploited user can bypass authentication to log in as administrator. The vulnerability affects TACAS+ feature of NFVIS due to incomplete validation of user input. Cisco has released advisory stating the patch is required to mitigate the vulnerability and no workaround is available for the same.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-g2DMVVh
Infected Technology	Cisco Enterprise NFVIS Release 4.5.1
Recommendation	Update to release 4.6.1
CVE-ID	CVE-2021-34746

Popular TP-Link router ships with vulnerable firmware

Description	
Check Point Research disclosed a vulnerability in WhatsApp that allowed attacker to extract sensitive information in the application's memory. Researcher found flaw in default firmware and web interface of TP-Link home series AC1200 Archer C50 router which allowed man-in-the-middle and denial of service attacks. The infected device ships with outdated version of firmware which matches 39 security flaws listed in MITRE database.	
Source	https://cybernews.com/security/amazon-tp-link-router-ships-with-vulnerable-firmware/?&web_view=true
Infected Technology	TP-Link AC1200 Archer C50 router (v6)
Recommendation	Update to the latest firmware

AMD chips are vulnerable to Meltdown-like attack

Description	
There have been new developments made by computer scientists at TU Dresden where AMD's Zen processor family is vulnerable to data-bothering meltdown-like attack. Meltdown as first disclosed in early 2018 and it is possible for allowing allowing malware running on a vulnerable computer or a rogue logged-in user to slowly figure out the contents of protected kernel memory and any secrets therein, such as keys and passwords.	
Source	https://www.theregister.com/2021/08/30/amd_meltdown_zen/?&web_view=true
Infected Technology	AMD CPU Chips
Recommendation	AMD recommends that SW vendors analyze their code for any potential vulnerabilities related to this type of transient execution.
CVE-ID	CVE-2020-12965

OpenSSL bugs impacts QNAP's NAS devices

Description	
QNAP's Network Attached Storage (NAS) awares their clients regarding to remote code execution (RCE) and denial-of-service (DOS) vulnerabilities patched by OpenSSL last week. The heap-based buffer overflow would likely lead to crashes but can also be abused by attackers for arbitary code execution.	
Source	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3711
Infected Technology	QNAP NAS device running QTS, QuTS hero, QuTScloud, and HBS 3 Hybrid Backup Sync
Recommendation	Apply OpenSSL OpenSSL 1.1.1l after release
CVE-ID	CVE-2021-3711 and CVE-2021-3712

Joker malware seen again

Description	
Joker virus has been again seen on Google play store impacting android devices. The infected apps is capable of entering contact and SMSes on infected devices. However, this malware is particularly dangerous because of its ability to subscribe victims to paid services. The joker operators seem to be highly active and innovative as they managed to bypass Google Play Store's defenses. Google has managed to remove infected apps from PlayStore but these apps are also being uploaded on third-party app store.	
Source	https://www.police.be/5998/fr/actualites/attention-le-virus-joker-est-de-retour-dans-lenvironnement-android
Infected Technology	Auxiliary Message, Element Scanner, Fast Magic SMS, Travel Wallpapers, Free CamScanner, Go Messages, Great SMS, and Super Message
Recommendation	Remove the mentioned apps from your android device(s)
CVE-ID	N/A

BrakTooth - Bluetooth users at risk

Description	
16 new security vulnerabilities dubbed as BrakTooth have been released by the ASSET Research Group. The vulnerabilities range from DOS via firmware crashes and deadlocks in commodity hardware to arbitrary code execution. As the affected vendors have been notified, some vendors have released the patch to close the vulnerabilities whereas others have confirmed that they are investigating the flaw or actively developing patches.	
Source	https://www.theregister.com/2021/09/01/braktooth_vulnerabilities_put_bluetooth_users/?&web_view=true
Infected Technology	Bluetooth
Recommendation	Apply the update once released by OEM Check the patch for CVEs listed in source domain
CVE-ID	CVE-2021-28139, CVE-2021-34144, CVE-2021-28136, CVE-2021-28135, CVE-2021-28155, CVE-2021-31717, CVE-2021-31609, CVE-2021-31612, CVE-2021-34150, CVE-2021-31613, CVE-2021-31611, CVE-2021-31785, CVE-2021-31786, CVE-2021-31610, CVE-2021-34149, CVE-

	2021-34146, CVE-2021-34143, CVE-2021-34145, CVE-2021-34148, CVE-2021-34147 and other pending CVEs

WebSVN Vulnerability abused by the new Mirai Variant

Description	
A new variant of Mirai has been affecting the command injection vulnerability of an open-source web application called WebSVN used for source code browsing. The malware was found to be used for launching DDoS attacks with a number of 8 possible attacks on different targets. The shell script can be further escalated to obtain additional details of the target environment. Linux binaries are being used for the attacks despite WebSVN supporting cross-platform.	
Source	https://cyware.com/news/new-mirai-variant-abuses-websvn-vulnerability-9bed48fc
Infected Technology	WebSVN
CVE-ID	CVE-2021-32305

Remote DoS against Apps Using Linphone SIP Stack

Description	
A vulnerability affecting the Linphone Session Initiation Protocol (SIP) allows adversaries to remotely crash applications. Analysis of the Linphone SIP client suite led to the discovery of the vulnerability in the Belle-sip library. To exploit the vulneravility remotely, an INVITE SIP request with specifically crafted From/To/Diversion header is sent to any client in the network. The request then triggers the NULL pointer dereference vulnerability. Any application that uses belle-sip under the hood to parse SIP messages is vulnerable and will crash upon receiving a malicious SIP 'call'.	
Source	https://www.securityweek.com/vulnerability-allows-remote-dos-attacks-against-apps-using-linphone-sip-stack?&web_view=true
Infected Technology	Linphone Session Initiation Protocol (SIP) client suite
Recommendation	Update to version 4.5.20
CVE-ID	CVE-2021-33056

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/