September 12, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Critical RCE Vulnerability Affects Zyxel NAS Devices — Firmware Patch Released
- Wordpress Vulnerability: High severity arbitrary file download/read vulnerability
- Cisco Releases Security Patches for New Vulnerabilities Impacting Multiple Products
- WordPress Core feature's six-year-old blind SSRF vulnerability may allow DDoS
- GIFShell attack creates reverse shell using Microsoft Teams GIFs

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.

Critical RCE Vulnerability Affects Zyxel NAS Devices — Firmware Patch Released	
Description	
Patches for a serious security hole affecting Zyxel's network-attached storage (NAS) devices have been published. According to a corporate alert published on September 6, "A format string vulnerability was discovered in a certain binary of Zyxel NAS systems, which might allow an attacker to gain unauthorized remote code execution through a forged UDP packet."The vulnerability affects the following versions: NAS326 (V5.21(AAZF.11)C0 and earlier), NAS540 (V5.21(AATB.8)C0 and earlier), and NAS542 (V5.21(ABAG.8)C0 and earlier). Hacking NAS devices is becoming a common practice. Zyxel previously addressed local privilege escalation and authenticated directory traversal vulnerabilities (CVE-2022-30526 and CVE-2022-2030). Attackers can take your sensitive and personal data if you don't take safeguards or keep the program updated. They even sometimes succeed in permanently erasing data.	
Source	https://thehackernews.com/2022/09/critical-rce-vulnerability-affects.html
Infected Technology	Zyxel NAS Devices NAS326, NAS540, and NAS542 models.
Recommendation	No security updates have been
CVE_ID	CVE-2022-34747

Wordpress Vulnerability: High severity arbitrary file download/read vulnerability

Description
In view of reports of active exploitation of a high severity arbitrary file download/read vulnerability, WordPress websites using BackupBuddy are being recommended to upgrade the plugin. Unauthenticated attackers might download any file stored on the server due to an insecure implementation of the technique used to retrieve locally stored files. A majority of observed attacks apparently attempted to read /etc/passwd, /wp-config.php, .my.cnf, or .accesshash files, which could be leveraged to further compromise victims, said Wordfence.

Source	https://portswigger.net/daily-swig/wordpress-warning-140k-backupbuddy-installations-on-alert-over-file-read-exploitation/
Infected Technology	Versions between 8.5.8.0 and 8.7.4.1
Recommendation	Update to latest patched version (8.7.5)
CVE_ID	CVE-2022-31474

Cisco Releases Security Patches for New Vulnerabilities Impacting Multiple Products

Description	
The network stack of NVIDIA Data Plane Development Kit (DPDK) has a vulnerability that results from improper error handling. A hacker might take advantage of this weakness by sending messages over the program interface. Using the Cisco Webex App, an unauthenticated attacker might alter links or other information and carry out phishing attacks. The device could reload or stop receiving traffic if an error condition is seen on the device interface.	
Source	https://thehackernews.com/2022/09/cisco-releases-security-patches-for-new.html
Infected Technology	NVIDIA Data Plane Development Kit (DPDK), Cisco SD-WAN vManage Software, Cisco Webex App, Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers
Recommendation	• Migrate to Cisco Small Business RV132W, RV160, or RV160W Routers • Update to the latest version for app
CVE_ID	CVE-2022-28199, CVE-2022-28199, CVE-2022-20696, CVE-2022-20863, CVE-2022-20923

WordPress Core feature's six-year-old blind SSRF vulnerability may allow DDoS

Description	
Security researchers at SonarSource disclosed a six-year-old blind server-side request forgery (SSRF) vulnerability in a WordPress Core feature that could allow distributed denial-of-service (DDoS) attacks. he flaw was first discovered in 2017, however it has not yet been fixed. The XMLRPC API, which is accessible via the xmlrpc.php file, exposes the pingback feature. This functionality could make it possible for attackers to launch DDoS assaults by purposefully requesting that hundreds of blogs check for pingbacks on a single victim server.	
Source	https://portswigger.net/daily-swig/six-year-old-blind-ssrf-vulnerability-in-wordpress-core-feature-could-enable-ddos-attacks
Infected Technology	WordPress CMS
Recommendation	All installations of WordPress with XMLRPC and pingback feature enabled

GIFShell attack creates reverse shell using Microsoft Teams GIFs	
Description	
Threat actors may utilize Microsoft Teams to launch unique phishing attacks and secretly carry out orders to collect data using... GIFs use a new attack method called "GIFShell. The main component of this attack is called 'GIFShell', which allows an attacker to create a reverse shell that delivers malicious commands vis base64 encoded GIFs in Teams, and exfiltrates the output through GIFs retrieved by Microsoft's own infrastructure. The attacker must first persuade a user to install a malicious stager that runs commands and uploads command output through a GIF url to a Microsoft Teams webhook to construct the reverse shell.	
Source	https://www.bleepingcomputer.com/news/security/gifshell-attack-creates-reverse-shell-using-microsoft-teams-gifs/
Infected Technology	Microsoft Teams
Recommendation	Update to latest version

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/