January 31, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Secret Backdoor in Dozens of WordPress Plugins and Themes
- CentOS Web Panel bug allows Remote Code Execution as root on Linux Servers
- Multiple Vulnerabilities Found in Cisco Redundancy Configuration Manager (RCM) for cisco StarOS Software
- North Korean Hackers Using Windows Update Service to Infect PCs with Malware

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.

Secret Backdoor in Dozens of WordPress Plugins and Themes

Description	
Dozens of WordPress themes and plugins were backdoored with the malicious code in 1st half of September 2021 with the goal of infecting further sites by the threat actors. The backdoor gave the attackers full administrative control over the websites that used 40 themes and 53 plugins belonging to AccessPress Themes, a Nepal Based company that boasts of no fewer than 360,000 active website installations. The infected extensions contained a dropper for a web shell that gives the attackers full access to the infected sites. The vulnerability has been assigned the CVE-2021-24867.	
Source	https://thehackernews.com/2022/01/hackers-planted-secret-backdoor-in.html
Infected Technology	Themes and Plugins developed by AccessPress Themes
Recommendation	AccessPress Themes and plugins should be upgrade immediately to a safe version from Official website or Wordpress[.]org
CVE_ID	CVE-2021-24867

CentOS Web Panel bug allows Remote Code Execution as root on Linux Servers

Description	
Multiple security vulnerabilities impacting Control Web Panel (CWP) are chained by unauthenticated attackers to gain remote code execution (RCE) as root on Linux servers. The two security flaws found are file inclusion vulnerability (CVE-2021-45467) and a file write (CVE-2021-45466) bug chained together that lead to RCE. CWP site claims that roughly 30,000 servers are running CWP in their infrastructure. According to BleepingComputer, they found almost 80,000 Internet-exposed CWP servers on BinaryEdge and over 200,000 can also be found on Shodan and Censys according to the researchers who discovered the pre-authentication RCE chain bug.	
Source	https://www.bleepingcomputer.com/news/security/cwp-bugs-allow-code-execution-as-root-on-linux-servers-patch-now/
Infected Technology	CWP software supported operating system such as CentOS, Rocky Linux, Alma Linux and Oracle Linux.
Recommendation	Recommended to update the CWP7+ version for operating systems from official vendor website (https://control-webpanel.com/changelog).
CVE_ID	CVE-2021-45467, CVE-2021-45466

Multiple Vulnerabilities Found in Cisco Redundancy Configuration Manager (RCM) for cisco StarOS Software

Description	
Multiple vulnerabilities in Cisco Redundancy (RCM) for Cisco StarOS Software could allow unauthenticated attacker to remotely disclose sensitive information or execute arbitrary commands on the configured container as the root. The vulnerabilities are not dependent on one another. The assigned CVEs are (CVE-2022-20649) for Cisco RCM Debug Remote Code Execution vulnerability and (CVE-2022-20648) for Cisco RCM Debug information Disclosure Vulnerability. In addition, a software release that is affected by one of the vulnerabilities may not be affected by the other vulnerability.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rcm-vuls-7cS3Nuq
Infected Technology	Cisco (RCM) Redundancy Configuration manager for StarOS Software.
Recommendation	Software Update released by Cisco addressing the vulnerabilities from vendor site.
CVE_ID	CVE-2022-20649, CVE-2022-20648

North Korean Hackers Using Windows Update Service to Infect PCs with Malware

Description	
The infamous Lazarus Group entertainer has been noticed mounting another mission that utilizes the Windows Update administration to execute its pernicious payload, extending the stockpile of living-off-the-land (LotL) procedures utilized by the APT gathering to additional its targets. The Lazarus Group, otherwise called APT38, Hidden Cobra, Whois Hacking Team, and Zinc, is the moniker relegated toward the North Korea-based country state hacking bunch that has been dynamic since no less than 2009. Last year, the danger entertainer was connected to an intricate social designing effort focusing on security specialists. "This is a fascinating procedure utilized by Lazarus to run its noxious DLL utilizing the Windows Update Client to sidestep security location systems," specialists Ankur Saini and Hossein Jazi noted. "With this strategy, the danger entertainer can execute its pernicious code through the Microsoft Windows Update Client."	
Source	https://thehackernews.com/2022/01/north-korean-hackers-using-windows.html
Infected Technology	Microsoft Windows
Recommendation	Update windows only from system settings

12-Year-Old Polkit Flaw Lets Unprivileged Linux Users Gain Root Access

Description

A 12-year-old security weakness has been revealed in a framework utility called Polkit that awards aggressors root honors on Linux frameworks, even as a proof-of-idea (PoC) exploit has arisen in the wild only hours after specialized subtleties of the bug became public.Dubbed "PwnKit" by online protection firm Qualys, the shortcoming impacts a part in polkit called pkexec, a program that is introduced of course on each significant Linux circulation like Ubuntu, Debian, Fedora, and CentOS.pkexec, closely resembling the sudo order, permits an approved client to execute orders as another client, serving as an option to sudo. In the event that no username is indicated, the order to be executed will be run as the regulatory super client, root. Polkit (formerly called PolicyKit) is a toolkit for controlling system-wide privileges in Unix-like operating systems, and provides a mechanism for non-privileged processes to communicate with privileged processes.

Source	https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034
Infected Technology	Ubuntu, Debian, Fedora, and CentOS.
Recommendation	Cybersecurity Help is currently unaware of any official solution to address this vulnerability.
CVE_ID	CVE-2021-4034

Windows vulnerability with new public exploits lets you become admin

Description	
A security researcher has publicly disclosed an exploit for a Windows local privilege elevation vulnerability that allows anyone to gain admin privileges in Windows 10. Using this vulnerability, threat actors with limited access to a compromised device can easily elevate their privileges to help spread laterally within the network, create new administrative users, or perform privileged commands. The vulnerability affects all supported support versions of Windows 10 before the January 2022 Patch Tuesday updates. multiple exploits were publicly released for CVE-2022-21882 that allow anyone to gain SYSTEM privileges on vulnerable Windows 10 devices. This means that their devices remain unprotected and vulnerable to an exploit that has historically been used in cyberattacks by APT hacking groups.	
Source	https://www.bleepingcomputer.com/news/microsoft/windows-vulnerability-with-new-public-exploits-lets-you-become-admin/
Infected Technology	Microsoft Windows 10
Recommendation	Strongly advised that admins install the updates rather than wait until
CVE_ID	CVE-2022-21882, CVE-2021-1732

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