February 21, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Critical Flaw Uncovered in WordPress Backup Plugin
- New Critical RCE Bug Found in Adobe Commerce, Magento
- New Linux Privilege Escalation Flaw Uncovered in snap package manager
- Attacker use Microsoft Teams as launchpad for malware
- Baby Golang-Based Botnet Already Pulling in $3K/Month for Operators

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 Flaw Uncovered in WordPress Backup Plugin

Description	
UpdraftPlus, a WordPress plugin with over three million installations, has a significant security vulnerability. A failed permissions-level check caused the vulnerability, allowing untrusted users access to backups. This flaw allowed any logged-in user on a WordPress installation with UpdraftPlus installed to download an existing backup – access that should have been limited to administrators only. In addition, the attacker can extract database credentials from a configuration file and successfully access the site database.	
Source	https://thehackernews.com/2022/02/critical-flaw-uncovered-in-wordpress.html
Infected Technology	WordPress Sites with UpdraftPlus 1.16.7 installed
Recommendation	Update to latest version (1.22.2 or 2.2.3 for premium version)
CVE_ID	CVE-2022-0633

New Critical RCE Bug Found in Adobe Commerce, Magento

Description	
Researchers have constructed a viable proof-of-concept (PoC) exploit for the recently fixed CVE-2022-24086 vulnerability, which was under active attack and led Adobe to provide an emergency patch last weekend. The new vulnerability has the same severity as its predecessor, which Adobe patched on February 13. CVE-2022-24087 has been assigned to it, and it is scored 9.8 on the CVSS vulnerability-scoring system.	
Source	https://threatpost.com/new-critical-rce-bug-found-in-adobe-commerce-magento/178554/
Infected Technology	Adobe Commerce, Magneto.
Recommendation	Update Adobe magneto with the latest security patches.
CVE_ID	CVE-2022-24086, CVE-2022-24087

New Linux Privilege Escalation Flaw Uncovered in snap package manager

Description	
Multiple security flaws have been discovered in Canonicals' Snap software packaging and deployment system, the most serious of which may be abused to get root privileges. The problem is caused by a privilege escalation flaw in the snap-confine function, which is used internally by snapd to create the execution environment for snap applications. If this vulnerability is successfully exploited, any unprivileged user can get root access on the affected system.	
Source	https://thehackernews.com/2022/02/new-linux-privilege-escalation-flaw.html
Infected Technology	Canonicals' Snap Software packaging and deployment system
Recommendation	Install the latest security patches.
CVE_ID	CVE-2021-44731

Attacker use Microsoft Teams as launchpad for malware

Description	
Hackers have realized that Microsoft Teams is an excellent tool for spreading tentacles throughout an organization's systems. In this generation of this attack, attackers attach .exe files to Teams chats. The file's name is now UserCentric.exe, but it may simply be altered to something more general and innocuous-sounding. The executable malware writes data to the Windows registry, installs DLL files, and generates shortcut links that enable the software to self-administer. It effectively allows attackers to get control of the victim's computer. Attackers can compromise a partner organization in order to listen in/on inter-organizational talks, or they can compromise an email address in order to get access to Teams.	
Source	https://nationalcybersecuritynews.today/hackers-caught-dropping-malware-into-microsoft-teams-chats-emailsecurity-phishing-ransomware/
Infected Technology	Microsoft Teams and System that downloaded the malware
Recommendation	Install sandbox to inspect all malicious content.

Baby Golang-Based Botnet Already Pulling in $3K/Month for Operators

Description	
Kraken is a new Golang-based botnet with a brawn that belies its youth: it uses the SmokeLoader malware loader to spread like wildfire and is now raking in a healthy USD $3,000 per month for its owners, according to researchers. At this point, Kraken can maintain persistence, collect information about the host, download and execute files, run shell commands, take screenshots, and steal various cryptocurrency wallets, including Zcash, Armory, Atomic, Bytecoin, Electrum, Ethereum, Exodus, Guarda and Jaxx Liberty.	
Source	https://threatpost.com/golang-botnet-pulling-in-3k-month/178509/
Infected Technology	Information and data of the host
Recommendation	Enable two-factor authentication for all organizational accounts to help mitigate phishing and credential stuffing attacks.

Project Zero researchers see promising trends in vulnerability fixes

Description	
According to a new assessment from Google's Project Zero, big IT companies are generally fixing significant bugs faster than they were three years ago. According to the data, Project Zero reported 376 concerns to vendors over a three-year period, with 350 of them — or 93.1 percent — being resolved. Most of the reports concern goods from three major vendors: Microsoft (26%), Apple (23%), and Google (23%). (16 percent). Project Zero bug reports "may be outliers" in that supplier know the defects will be disclosed within a predetermined period, and also because "Project Zero is a trusted source of dependable bug reports," according to the group's data.	
Source	https://www.cyberscoop.com/project-zero-bug-fixes-data/
Infected Technology	Big Tech Vendors
Recommendation	Do not download anything from suspicious websites.

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/