October 17, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- GitLab patches RCE bug in GitHub import function
- Adobe patches critical Magento XSS that puts sites at takeover risk.
- New Ducktail Malware hijacks Facebook business accounts
- NPM's registry API vulnerable to timing attack
- Trojan version of WhatsApp caught infecting Android Devices
- Source code Alder BIOS leaded

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.

GitLab patches RCE bug in GitHub import function

Description
Attackers were able to launch multiple attacks on GitLab servers, including the cloud hosted GitLab.com platform. A vulnerability in the way GitLab imports data from GitHub might be leveraged to execute instructions on the host server. An attacker might use the command injection vulnerabilities on standalone GitLab installations to advance from Redis to Bash and issue commands to the operating system. Any possible attacker would have access to the host with privileges of the host process through remote code execution (RCE). The exploit might be used by an attacker with a standalone GitLab installation and an API access token to steal data, inject malicious code, and carry out other illegal acts against GitLab.com.

Source	https://portswigger.net/daily-swig/gitlab-patches-rce-bug-in-github-import-function
Infected Technology	GitHub import function
Recommendation	• Upgrade GitLab installation
CVE_ID	CVE-2022-2884

Adobe patches critical Magento XSS that puts sites at takeover risk.

Description
A super-critical vulnerability in Adobe Magento could allow attackers to fully compromise e-commerce platforms, according to the security researcher who unearthed the bug. Adobe has urged users to update their systems to protect their websites from abuse of the flaw, which has been assigned the maximum possible severity (CVSS) score of 10. The stored cross-site scripting (XSS) bug can lead to arbitrary code execution, according to an Adobe security advisory published on October 11. The flaw affects versions 2.4.4-p1 and earlier, as well as 2.4.5 and earlier, of Adobe Commerce and Magento Open Source. The issue has been patched in versions 2.4.5-p1 and 2.4.4-p2.

Source	https://portswigger.net/daily-swig/adobe-patches-critical-magento-xss-that-puts-sites-at-takeover-risk
Infected Technology	Adobe Magento
Recommendation	• Upgrade to the latest version and patch the flaw as soon as possible.
CVE_ID	CVE-2022-35698

New Ducktail Malware hijacks Facebook business accounts

Description	
Ducktail, an information stealing malware, is now actively being distributed in PHP version. The new malware is now distributed in forms of cracker for legitimate applications. The PHP version, like its predecessor exfiltrates sensitive information saved in browsers. The trojan is using file sharing services such as mediafire for distribution and exfiltrates data in form of JSON to newly hosted websites to evade detection	
Source	https://www.zscaler.com/blogs/security-research/new-php-variant-ducktail-infostealer-targeting-facebook-business-accounts
Attack Vector	Phishing
Recommendation	Do not download applications from untrusted source Do not click on suspicious links

NPM's registry API vulnerable to timing attack

Description	
A new timing attack has been identified in NPM's registry API which can be exploited to disclose private packages used by an organization. The disclosure of the information makes the target organization prone to supply chain threat where vulnerability in the disclosed packets can be used to initiate an attack. The attack analyzes the time difference between 404 responses returned by npm's registry API. The vulnerability has been disclosed to GitHub however cannot be fixed due to architectural limitation.	
Source	https://blog.aquasec.com/private-packages-disclosed-via-timing-attack-on-npm
Infected Technology	NPM registry API
Recommendation	• Routinely scan NPM and other package management platform for spoofed packages • Actively monitor public assets to identify recon activity

Trojan version of WhatsApp caught infecting Android Devices

Description	
YoWhatsApp, an unofficial version of WhatsApp, has been used to deploy a trojan named Triada. The malware is to steal the keys WhatsApp that can be used to use the service without application. The malicious version of the application offers ability to lock chat, send messages to unsaved numbers and customization. The malicious code has been identified by Kaspersky Labs in YoWhatsApp version 2.22.11.75. A successful theft of the key can lead to total compromise of the account.	
Source	https://securelist.com/malicious-whatsapp-mod-distributed-through-legitimate-apps/107690/
Infected Technology	YoWhatsApp
Recommendation	Do not download application from unofficial sources

Source code Alder BIOS leaded

Description	
Intel has confirmed that their propriety source code for its Alder Lake CPU has been leaked and released online. The leaked content contains UEFI code for Alder Lake launched in November of 2021. According to Intel, the leaked information, however, does not contain vulnerabilities that can be used by the threat vector to exploit the customers using the leaked version of the BIOS.	
Source	https://www.tomshardware.com/news/intel-confirms-6gb-alder-lake-bios-source-code-leak-new-details-emerge
Infected Technology	Intel

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/