March 14, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Critical Bugs Could Let Attackers Remotely Hack, Damage APC Smart-UPS Devices
- Dirty Pipe Local Privilege Escalation
- 2 New Mozilla Firefox 0-Day bug under active attack.
- Adobe Patches 'Critical' Security Flaws in Illustrator, After Effects
- SQL injection identified in Moodle

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, Bug Crowd, under armor, 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 Bugs Could Let Attackers Remotely Hack, Damage APC Smart-UPS Devices

Description	
Three high-impact security vulnerabilities have been discovered in APC Smart-UPS systems, which could also be exploited as a physical weapon by remote attackers to gain unauthorized access and control. The weaknesses, collectively known as TLStorm, "enable for total remote control of Smart-UPS equipment and the capacity to carry out serious cyber-physical attacks," according to the researchers. In mission-critical locations such as medical centers, server rooms, and industrial systems, uninterruptible power supply (UPS) devices act as emergency backup power suppliers. "By using RCE vulnerability attackers were able to bypass the software protection and let the current spike periods run over and over until the DC link capacitor heated up to ~150 degrees Celsius (~300F), which caused the capacitor to burst and brick the UPS in a cloud of electrolyte gas, causing collateral damage to the device."	
Source	https://thehackernews.com/2022/03/critical-bugs-could-let-attackers.html
Infected Technology	APC Smart-UPS Devices
Recommendation	Install latest updates for reducing the risk of successful exploitation of these vulnerabilities.
CVE_ID	CVE-2022-22805, CVE-2022-22806, CVE-2022-0715

Dirty Pipe Local Privilege Escalation

Description	
A vulnerability within the Linux kernel since version 5.8 allows overwriting data in arbitrary read-only files. This leads to privilege escalation because unprivileged processes also can inject code into root processes. This local privilege escalation is similar but easy to take advantage of than previously released CVE-2016-5195 “Dirty Cow”. Security researcher Max Kellermann responsibly disclosed the ‘Dirty Pipe’ vulnerability and stated that it affects Linux Kernel 5.8 and later versions, even on Android devices.	
Source	https://medium.com/cryptogennepal/dirty-pipe-cve-2022-0847-b7c0e7b3b3e0
Infected Technology	Linux kernel since 5.8 before 5.17rc
Recommendation	Update the Linux kernel to latest version
CVE_ID	CVE-2022-0847

2 New Mozilla Firefox 0-Day bug under active attack.

Description	
On 5/11/ 2022, Mozilla has released a software update to its Firefox Web browser to contain a high-impact security vulnerability, which is being exploited in the wild. The zero-day vulnerabilities are described as use-after-free issues that affect the parameter processing of the Extensible Stylesheet Language Transformations (XSLT) and the WebGPU inter-process communication (IPC) Framework, which could be exploited to corrupt valid data and execute arbitrary code on compromised systems – stem mainly from a "confusion over which part of the program is responsible for freeing the memory."	
Source	https://thehackernews.com/2022/03/2-new-mozilla-firefox-0-day-bugs-under.html
Infected Technology	Firefox 97.0.2 Firefox ESR 91.6.1 Firefox for Android 97.3.0 Focus 97.3.0 Thunderbird 91.6.2
Recommendation	Update the patch and upgrade to the new Mozilla Firefox browser.
CVE_ID	CVE-2022-26485 CVE-2022-26486

Adobe Patches 'Critical' Security Flaws in Illustrator, After Effects

Description	
Adobe Illustrator, a prominent vector graphics design program available for both macOS and Windows platforms, was patched for the most serious of the flaws. Adobe categorized the Illustrator problem as "critical" with a CVSS base score of 7.8 in an advisory. The CVE-2022-23187 flaw is a buffer overflow that affects Illustrator 2022 version 26.0.3 (and older versions) on both Windows and macOS platforms, according to Adobe.	
Source	
Infected Technology	Adobe Illustrator vulnerability on Windows and macOS.
Recommendation	• Upgrade Illustrator 2022 to later version or above version 26.1.0.
CVE_ID	CVE-2022-23187

SQL injection identified in Moodle

Description	
An SQL injection vulnerability was discovered in Moodle, an e-learning platform. Many institutions rely on Moodle and this vulnerability could allow adversaries to obtain sensitive information of the faculty and students. Although the malicious actor needs a teacher's credentials to perform this attack, it allows them unauthorized access to the database and potentially take control over it. The SQLi vulnerability can provide a foothold that could be used to mount further sophisticated attacks such as stored XSS.	
Source	https://portswigger.net/daily-swig/sql-injection-vulnerability-in-e-learning-platform-moodle-could-enable-database-takeover
Infected Technology	Moodle e-learning platform
Recommendation	• The researcher published the proof of concept without informing Moodle, however, Moodle have prepared a patch for the vulnerability and is scheduled to be made available from 14th March 2022.

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/