December 20, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Firefox Fixes Password leak via Windows cloud Clipboard Feature
- Microsoft Released Windows Update to Patch Zero-Day Used to Spread Emotet Malware
- New Patch Released for Second Log4j Vulnerability
- Lenovo laptops vulnerable to privilege elevation bug
- New Local Attack Vector Expands the Attack Surface of Log4j Vulnerability

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.

Firefox Fixes Password leak via Windows cloud Clipboard Feature	
Description	
Mozilla has fixed an issue related with Windows Cloud Clipboard that records the username and passwords of the Firefox browser, which is categorized as a severe security risk that could have exposed Credentials to non-owners whenever users copied or cut a password. Mozilla releases the fix in the Firefox 94. Talking about a bug, it was related to a feature known as Windows Cloud Clipboard, that allows users to sync their local clipboard history to their accounts. This clipboard feature was disabled by default, but enabling it once will allow users to access the cloud clipboard section by pressing the WINDOWS+V shortcut key which grants users access to clipboard data from all devices. Although the feature is useful allowing users to surf through past items they copied or cut and re-paste the same data. Mozilla has announced they have now modified the Firefox browser which won't be storing the usernames and passwords copied from the browser's password section, instead it will be stored locally. As an additional Protection, Mozilla has said in Private Browsing windows copied data will not be synced to the Windows Cloud Clipboard.	
Source	https://therecord.media/firefox-fixes-password-leak-via-windows-cloud-clipboard-feature/
Infected Technology	Firefox Browser Below 94 Version
Recommendation	• Update Firefox Browser to the latest version.

Microsoft Released Windows Update to Patch Zero-Day Used to Spread Emotet Malware

Description	
Microsoft has released a patch addressing multiple security vulnerabilities in Windows & others software. Among many other vulnerabilities one of the most critical was actively exploited flaw that is being used to deliver malware such as Emotet, TrickBot or Bazaloader. It is a Windows AppX installer spoofing vulnerability that could to be exploited to achieve arbitrary code execution. Its impact could be low on users whose accounts are configured to have fewer user rights on the system comparing the users who operates with administrative user rights. The released patch also comes with the remediations for 10 remote code execution flaws affecting different Microsoft Based Products.	
Source	https://thehackernews.com/2021/12/microsoft-issues-windows-update-to.html?m=1
Infected Technology	Microsoft Windows
Recommendation	• Update the Windows for newly released security patches by Microsoft.
CVE_ID	CVE-2021-43890

New Patch Released for Second Log4j Vulnerability

Description	
Apache software Foundation has released out a new fix for the Log4J logging utility after the previous patch for the Log4Shell exploit was considered as incomplete in certain non-default configurations. The second log4j Vulnerability affects all the versions of Log4j from 2.0-beta9 up to 2.15.0. Due to the incomplete patch for a previous critical remote code execution vulnerability that can be abused to infiltrate and compromise the systems. The second Log4j vulnerability could be abused by supplying malicious input data as a JNDI Lookup pattern which results in Denial-of-service (DOS) attack. The patch was released for the second Log4j vulnerability in the latest version of Log4j 2.16.0(for users requiring java 9 or later) which removes support for message lookups and disables JNDI by default. It is also recommended to users requiring Java 7 to upgrade Log4j 2.12.2 When it becomes available to users.	
Source	https://thehackernews.com/2021/12/second-log4j-vulnerability-cve-2021.html?&web_view=true
Infected Technology	Apache Software Foundation Log4j Library 2.15.0 versions.
Recommendation	• Update to the newly released Log4j 2.16.0 version by Apache software Foundation.
CVE_ID	CVE-2021-45046

Lenovo laptops vulnerable to privilege elevation bug	
Description	
ImControllerService component within Lenovo System Interface Foundation is vulnerable which allows the attacker to perform privilege elevation and execute commands with admin privileges. The privilege elevation bug is assigned with CVE-2021-3922 and CVE-2021-3969 affects the component within the versions below 1.1.20.3. The vulnerabilities were reported to Lenovo by the researchers at NCC on 29th October 2021 and the security updates were released on November 17, 2021 while relevant advisory was published on December 14, 2021.	
Source	https://www.bleepingcomputer.com/news/security/lenovo-laptops-vulnerable-to-bug-allowing-admin-privileges/
Infected Technology	Lenovo Desktops/Laptops running 1.1.20.2 or older versions of Im Controller component
Recommendation	Update the Im Controller to the latest version (1.1.20.3)
CVE_ID	CVE-2021-3922 and CVE-2021-3969

New Local Attack Vector Expands the Attack Surface of Log4j Vulnerability	
Description	
Latest Local Attack Vector expanding Attack Surface of Log4jSecurity researchers have identified the new attack vector for exploiting the Log4Shell vulnerability on servers using the JavaScript WebSocket connection locally. This newly identified attack vector explains that anyone with the vulnerable Log4j version on the network can trigger the vulnerability just by browsing the website. This attack vector expands the attack surface and also impacts the services running internally and which aren't even exposed to the internet. The CTO and co-founder of the IR firm in BreachQuest explained that there's no surprise when additional vulnerabilities are discovered in Log4j as the focus of the entire cyber security community is on the library. Also, the newly vulnerabilities being discovered in Log4j is making the Log4j library more secure as the attention is focused towards it by the community.	
Source	https://thehackernews.com/2021/12/new-local-attack-vector-expands-attack.html
Infected Technology	• Software using Log4j Library
Recommendation	Patch to new version 2.17.0
CVE_ID	CVE-2021-44228

Update Google Chrome to patch New Zero-Day Exploit Detected in the Wild

Description	
Google has released patches for five security flaws in its chrome web browser, including one that it claims is being exploited in the wild, making it the 17th such flaw to be discovered since the beginning of the year. As of now, it's unclear how the flaw is being used in real-world assaults, but Google published a brief statement saying, "it's aware of claims that an exploit for CVE-2021-4102 exists in the wild." This is done to guarantee that most users are updated with a remedy and to prevent future exploitation by other threat actors.	
Source	https://thehackernews.com/2021/12/update-google-chrome-to-patch-new-zero.html
Infected Technology	Google Chrome
Recommendation	Update the latest patch available.
CVE_ID	CVE-2021-4102

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/