May 23, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- SharePoint RCE bug resurfaces again after being patched by Microsoft
- High-Severity Bug Reported in Google's OAuth Client Library for Java
- Citical Jupiter WordPress plugin flaws let hackers take over sites
- Hackers Trick Users with Fake Windows 11 Downloads to Distribute Vidar Malware
- Smart Locks and BLE devices Vulnerable to Bluetooth relay attacks

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.

SharePoint RCE bug resurfaces again after being patched by Microsoft

Description	
A security researcher discovered a new approach to perform remote code execution (RCE) attacks using a newly fixed deserialization issue in Microsoft SharePoint. The vulnerability, which is a variation of one that was fixed in February, exploits SharePoint's site creation functionality to upload and run malicious files on the server. To send complicated objects to servers and between processes, several languages employ serialization and deserialization. If the deserialization process is vulnerable, an adversary can use it to submit malicious objects to the server and have them run.	
Source	https://portswigger.net/daily-swig/sharepoint-rce-bug-resurfaces-three-months-after-being-patched-by-microsoft
Infected Technology	Sharepoint Version lower than 16.0.14931.20286
Recommendation	Update to Latest Patched Version
CVE_ID	CVE-2022-22005

High-Severity Bug Reported in Google's OAuth Client Library for Java

Description	
Last month, Google patched a critical weakness in its Java OAuth client library that could be exploited by a malicious actor with a compromised token to deliver arbitrary payloads. The severity of the vulnerability is 8.7 out of ten, and it involves an authentication bypass in the library caused by incorrect cryptographic signature verification. The open-source Java library, which is based on the Google HTTP Client Library for Java, allows users to get access tokens from any online service that supports the OAuth authorization standard.	
Source	https://thehackernews.com/2022/05/high-severity-bug-reported-in-googles.html
Infected Technology	google-OAuthjava-client library
Recommendation	Update to version 1.33.3
CVE_ID	CVE-2021-22573

Citical Jupiter WordPress plugin flaws let hackers take over sites

Description	
A set of critical vulnerabilities were discovered by security analyst of WordPress which was impacting the Jupiter Theme and JupiterX core plugins, and among them privilege escalation flaw was critical. The vulnerability was tracked as CVE-2022-1654 and given a CVSS score of 9.9 because the vulnerability allows any authenticated user on a site using the vulnerable plugins to gain administrative privileges. And after exploitation attacker can alter the contents of WordPress, inject malicious scripts, or can delete the contents too.	
Source	https://www.bleepingcomputer.com/news/security/critical-jupiter-wordpress-plugin-flaws-let-hackers-take-over-sites/
Infected Technology	WordPress
Recommendation	Update to latest version
CVE_ID	CVE-2022-1654

Hackers Trick Users with Fake Windows 11 Downloads to Distribute Vidar Malware

Description	
To infect devices with the Vidar information stealer virus, fraudulent websites posing as Microsoft's Windows 11 download center are attempting to deceive users into downloading trojanized installation packages. The fake sites were developed to distribute malicious ISO files that infect endpoints with the Vidar info-stealer. The C2 configuration is retrieved by these Vidar malware versions through attacker-controlled social media channels on the Telegram and Mastodon networks. In addition, the cybersecurity firm cautioned that the threat actor behind the impersonation campaign is also leveraging backdoored versions of Adobe Photoshop and other legitimate software such as Microsoft Teams to deliver Vidar malware.	
Source	https://thehackernews.com/2022/05/hackers-trick-users-with-fake-windows.html
Infected Technology	Windows
Recommendation	Download from valid official websites

Smart Locks and BLE devices Vulnerable to Bluetooth relay attacks

Description	
Bluetooth Low Energy (BLE) is a wireless technology that is used for authentication of Bluetooth devices in a close proximity. A vulnerability in the current implementation of BLE has made it easy for attackers to unlock and operate cars, unlock residential smart locks, and breach secure areas more easily. NCC group, a U.K. based Cybersecurity company said “An attacker can falsely indicate the proximity of BLE devices to one another using relay attacks. This may enable unauthorized access to devices in BLE-based proximity authentication systems.” Although many theoretical methods to prevent relay attacks exist, the Bluetooth Special Interest Group (SIG) have not implemented them and are currently working on “more accurate ranging mechanisms”	
Source	https://thehackernews.com/2022/05/new-bluetooth-hack-could-let-attackers.html
Infected Technology	BLE devices
Recommendation	Wait for Official Patch

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/