February 14, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- RCE flaws in “PHP Everywhere” plugin affecting thousands of wordpress sites
- Google Fixes Remote privilege escalation flaw on Android
- Microsoft blocks the Office Macros from internet by default
- Microsoft released patch for Prominent vulnerabilities
- Command Injection vulnerability in Totolink Firmware 9.1.0U.6118B2021102

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.

RCE flaws in “PHP Everywhere” plugin affecting thousands of wordpress sites

Description	
A wordpress plugin known as PHP Everywhere have critical security vulnerabilities disclosed affecting more than 30,000 websites all over the world. Disclosed vulnerabilities allows an attacker to execute the arbitrary code on the affected systems. Installing PHP Everywhere plugin in wordpress enables users to insert and execute PHP-based code in the CMS pages, Posts and sidebar. The disclosed issues are Remote Code Execution by subscriber + users via shortcode (CVE-2022-24663), Remote Code Execution by Contributor + users via metabox (CVE-2022-24664) and Remote code Execution by Contributor+ users via Gutenberg block (CVE-2022-24665). The successful exploitation of these three vulnerabilities results in the malicious PHP code execution which can be leveraged to complete site takeover.	
Source	https://thehackernews.com/2022/02/critical-rce-flaws-in-php-everywhere.html
Infected Technology	“PHP Everywhere” Plugin installed WordPress based websites.
Recommendation	• Updating to the latest released plugin version 3.0. • Users relying on Classic Editor instead of Block Editor are recommended to uninstall the plugin and download alternative solution to host custom PHP code.
CVE_ID	CVE-2022-24663, CVE-2022-24664, CVE-2022-24665

Google Fixes Remote privilege escalation flaw on Android	
Description	
Google has released the security updates on android, addressing the two security flaws, one being major that cause remote escalation of privilege that requires no user interaction. The vulnerability was assigned CVE-2021-38675, and it affects the latest Android 12 version. Another flaw was also addressed on the update is CVE-2021-30317, which affects the closed-source component of Qualcomm and concerns only Android devices that use vendor's hardware.	
Source	https://www.bleepingcomputer.com/news/security/google-fixes-remote-escalation-of-privileges-bug-on-android/
Infected Technology	Google's Android Operating system version 12
Recommendation	• Recommended to follow official security updates by Google
CVE_ID	CVE-2021-39675, CVE-2021-30317

Command Injection vulnerability in Totolink Firmware 9.1.0U.6118B2021102	
Description	
The method UploadFirmwareFile in TOTOLINK X5000R v9.1.0u.6118 B20201102 was determined to have a command injection vulnerability. This vulnerability allows attackers to run arbitrary commands via the parameter host_time. This vulnerability was assigned the CVE-2021-45742 with the CVSS 3.1 Base score 9.8.	
Source	https://cyber.vumetric.com/vulns/CVE-2021-45733/command-injection-vulnerability-in-totolink-x5000r-firmware-9-1-0u-6118b20201102/
Infected Technology	Totolink X5000R Firmware v9.1.0u.6118B20201102
Recommendation	• Follow the official firmware vendor notice for the patch of the vulnerability.
CVE_ID	CVE-2021-45733

Microsoft blocks the Office Macros from internet by default

Description	
Microsoft has announced the Macro code from the internet will be turned off by default. In past, Macro coding languages both Microsoft developed scripting language wordbasic and another language Visual Basic for Applications (VBA) was widely abused by the malware writers to create macro viruses. With the time people exchanged office documents frequently a day, macro viruses quickly become an ever-present problem. According to Microsoft, from now on any document tagged as having come from internet (e.g: an email attachment or a web download, will be treated as though it contains no macros. By default, users won't be able to enable the macros from inside office, even if convinced that macros are both expected and trustworthy.	
Source	https://nakedsecurity.sophos.com/2022/02/08/at-last-office-macros-from-the-internet-to-be-blocked-by-default/
Infected Technology	Microsoft Office Products
Recommendation	• Recommended to follow the Microsoft official the update guide regarding macros blocked by default in office products.

Microsoft released patch for Prominent vulnerabilities	
Description	
Microsoft published its monthly security update on Tuesday, uncovering 51 vulnerabilities in its diverse range of hardware and software. None of the vulnerabilities identified this month are classified as “critical” which is unusual for the company’s Patch Tuesdays. Furthermore, none of the vulnerabilities that Microsoft addressed has been exploited in the wild, nor they have been publicly published. However, there are few noteworthy vulnerabilities, including CVE-2022-21997, CVE-2022-21999, and CVE-2022-22715, all of which are privilege escalation flaws in the Microsoft print spooler service. In the case that an exploit is created, an adversary might exploit these flaws to execute code as a system user or with higher-level privileges.	
Source	https://blog.talosintelligence.com/2022/02/microsoft-patch-tuesday-for-feb-2022.html
Infected Technology	Microsoft Based Products.
Recommendation	Follow the monthly security update released by Microsof
CVE_ID	CVE-2022-21997, CVE-2022-21999, CVE-2022-22715

Apple Patches Actively Exploited WebKit Zero Day	
Description	
A memory issue influences heap iPhone, iPad and MacOS gadgets and permits assailants to execute erratic code in the wake of handling vindictive web content. Macintosh has fixed one more zero-day weakness, this time in its WebKit program motor, that danger entertainers as of now are effectively taking advantage of to think twice about, iPads and MacOS gadgets. On account of Apple's zero-day, danger entertainers can execute erratic code on impacted gadgets after they process noxiously created web content, the organization said in a portrayal of the bug. The imperfection likewise can prompt startling OS crashes.	
Source	https://threatpost.com/apple-patches-actively-exploited-webkit-zero-day/178370/
Infected Technology	Apple Based Products iphone, iPad, MacOS
Recommendation	Installing the OS 15.3.1 and iPad OS 15.3.1 updates will protect your device, though it does need to be connected to a Wi-Fi network in order to install the patch.
CVE_ID	CVE-2022-22620 , CVE-2022-22587 CVE-2022-22594

Fake Windows 11 upgrade installers infect you with RedLine malware	
Description	
Threat actors have started distributing fake Windows 11 upgrade installers to users of Windows 10, tricking them into downloading and executing RedLine stealer malware. The circumstance of the assaults corresponds with the second that Microsoft declared Windows 11's expansive sending stage, so the attacker was totally ready for this move and trusted that the right second will augment their activity's prosperity. RedLine stealer is presently the most generally conveyed password, browser cookie, Mastercard, and cryptographic money wallet information grabber, so its diseases can have desperate ramifications for the people in question. The site appears like a genuine Microsoft site and, if the visitor clicked on the 'Download Now' button, they received a 1.5 MB ZIP archive named "Windows11InstallationAssistant.zip," fetched directly from a Discord CDN.	
Source	https://www.bleepingcomputer.com/news/security/fake-windows-11-upgrade-installers-infect-you-with-redline-malware/
Infected Technology	Microsoft Windows 11 Operating System
Recommendation	• Recommended to upgrade to windows 11 via the official Microsoft site.

Hackers Planted Fake Digital Evidence on Devices of Indian Activists and Lawyers	
Description	
A formerly obscure hacking group has been connected to designated assaults against common liberties activists, basic freedoms protectors, scholastics, and legal advisors across India trying to plant "implicating advanced proof.""ModifiedElephant works using monetarily accessible remote access trojans (RATs) and has expected connections to the business reconnaissance industry," the analysts said. "The danger entertainer utilizes skewer phishing with malignant records to convey malware, like NetWire, DarkComet, and basic keyloggers.	
Source	https://thehackernews.com/2022/02/hackers-planted-fake-digital-evidence.html
Infected Technology	Digital Devices of Indian activists and lawyers
Recommendation	• Recommended not to click the received email without verifying it source.

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/