May 24
2021

INFOSEC WEEKLY

#MADE4SECURITY

- Android patches four zer0-day exploits
- MountLocker Ransomware worms through using Windows API
- Object Injection Vulnerability Affects WordPress Versions 3.7 to 5.7.1
- Fake Microsoft Authenticator extension discovered in Chrome Store
- Blind SQL Injection flaw in WP Statistics impacted 600+ sites
- Heap-based buffer overflow in Google Chrome could lead to code execution
- Rapid7 Source Code Breached in Codecov Supply-Chain Attack

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.

1. Android patches four zero-day exploits

Description	
Google's Project Zero team has patched four Android security vulnerabilities. The zero-day vulnerabilities were exploited in the wild but only impacted a limited number of users according to Google. The attacker attempted to exploit the flaws that impacted Qualcomm GPU and Arm Mali GPU Driver Components. The successful exploitation of the vulnerability was possible by crafting a malicious file to the target host. The remote-based attackers were able to execute arbitrary malicious code within the privileged process of the vulnerable user. The attackers were able to access the text message, call history and listen to the conversation of the vulnerable user.	
Source	https://source.android.com/security/bulletin/2021-05-01
Infected Technology	Android OS
CVE ID	CVE-2021-1905, CVE-2021-1906, CVE-2021-28663 CVE-2021-28664
Recommendation	Update the Android OS to the latest available version

2. MountLocker Ransomware worms through using Windows API

Description	
MountLocker is a Ransomware-as-a-Service (RaaS) developed by a team of developers. The developers create malicious code to install ransomware on software and payment sides, ultimately hacking the business and encrypting the target devices. The group 'XingLocker' have customized the MountLocker ransomware feature by running the worm feature sample in the Windows command line with /NETWORK argument. The MountLocker used the Windows Active Directory Service Interfaces API as a part of its worm feature. The worm retrieved the domain controller names. Once connected to the Active Directory service, the worm iterated over the databases. The ransomware executable will be copied to the remote devices that will facilitate MountLocker to encrypt the target devices.	
Source	https://www.bleepingcomputer.com/news/security/mountlocker-ransomware-uses-windows-api-to-worm-through-networks/
Infected Technology	Microsoft Windows

3. Object Injection Vulnerability Affects WordPress Versions 3.7 to 5.7.1

Description	
According to WPScan, the new object injection vulnerability is due to versions of PHPMailer library between 6.1.8 and 6.4. The vulnerability occurs when user-supplied input is not properly sanitized before being passed to the unserialize() PHP function. Since PHP allows object serialization, attackers could pass ad-hoc serializes strings to a vulnerable unserialize() call, resulting in an arbitrary PHP object injection into the application scope. The ramification of such an attack is that it allows attacker to perform different kinds of malicious attacks, such as Code Injection, SQL Injection, Path Traversal, and Application Denial of Service, depending on the context. Fortunately, as per secure.net, WordPress doesn't allow direct access to PHPMailer as all that is done through the WordPress API, where extra protections are in place. Nevertheless, this could be a good example of vulnerability going undetected and amplified over time after it is used together with other vulnerabilities.	
Source	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36326
Infected Technology	WordPress versions 3.7 to 5.7.1
CVE ID	CVE-2020-36326
Recommendation	Consider updating WordPress version => 5.7.2

4. Fake Microsoft Authenticator extension discovered in Chrome Store

Description	
An extension using both the name and branding of the legitimate Microsoft Authenticator app was discovered in the browser add-on marketplace and managed to accrue a three out of five-star rating. This fake Microsoft Authenticator extension was made available on April 23 after failing to be spotted by Google's security systems and has reached 448 users. The name suggests that it is an official product by Microsoft, but it is not. One hint that something is off is that the company that is offering the extension is not Microsoft Corporation but "Extensions".	
Source	https://www.ghacks.net/2021/05/18/dont-download-this-microsoft-authenticator-extension-for-chrome-it-is-fake/
Infected Technology	Google Chrome
Recommendation	Properly inspect before download and installing

5. Blind SQL Injection flaw in WP Statistics impacted 600+ sites	
Description	
Researches from the Wordfence Threat Intelligence discovered a Time-Based Blind SQL Injection vulnerability in WP Statistics, which is a WordPress plugin with over 600,000 active installs. The vulnerability could be exploited by an unauthenticated attacker to extract sensitive information from a WordPress website using the vulnerable plugin. While the "Page" menu item of WP Statistics, was intended for admins only and would not display information to non-admin users, it was possible to start loading this page's construction by sending a request to wp-admin/admin.php with the page parameter set to wps_pages_page.	
Source	https://www.wordfence.com/blog/2021/05/over-600000-sites-impacted-by-wp-statistics-patch/?utm_content=167209759&utm_medium=social&utm_source=twitter&hss_channel=tw-609853517
Infected Technology	WordPress Plugin version < 13.0.8
CVE ID	CVE-2021-24340
Recommendation	Consider upgrading the vulnerable plugin to the patched version 13.0.8 or later.

6. Heap-based buffer overflow in Google Chrome could lead to code execution	
Description	
Cisco Talos recently discovered an exploitable heap-based buffer overflow vulnerability in Google Chrome. TALOS-2021-1235 (CVE-2021-21160) is a buffer overflow vulnerability in Chrome's AudioDelay function that could allow an adversary to execute remote code. An attacker could exploit this vulnerability by tricking a user into visiting a specially crafted HTML page in Chrome. Proper heap grooming can give the attacker full control of this heap overflow vulnerability, and as a result, could allow it to be turned into arbitrary code execution.	
Source	https://blog.talosintelligence.com/2021/05/vuln-spotlight-google-chrome-heap.html?&web_view=true
Infected Technology	Google Chrome, versions 841401 (89.0.4383.0, 64-bit) and 844161 (90.0.4390.0, 64-bit)
CVE ID	CVE-2021-21160
Recommendation	update these affected products as soon as possible

7. Rapid7 Source Code Breached in Codecov Supply-Chain Attack	
Description	
Cybersecurity company Rapid7 on Thursday revealed that unidentified actors improperly managed to get hold of a small portion of its source code repositories in the aftermath of the software supply chain compromise targeting Codecov earlier this year. According to the company, the actor gained access because of an error in Codecov's Docker image creation process that allowed the actor to extract the credential required to modify our Bash Uploader script. Rapid7 reiterated there's no evidence that other corporate systems or production environments were accessed, or that any malicious changes were made to those repositories. The company also added its use of the Uploader script was limited to a single CI server that was used to test and build some internal tools for its MDR service.	
Source	https://www.rapid7.com/blog/post/2021/05/13/rapid7s-response-to-codecov-incident/
Infected Technology	Rapid 7 Source Code Repository

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/