June 13
2021

INFOSEC WEEKLY

#MADE4SECURITY

- A new zero-day Bug in Chrome
- Samsung pre-installed apps are exploited for spying
- Dual vulnerability combo in popular CMS Joomla could lead to 'full system compromise'
- Microsoft patches six Windows zero-days, including a commercial exploit
- Adobe Patches Major Security Flaws in PDF Reader, Photoshop
- Microsoft Office MSGraph vulnerability could lead to code execution
- Intel fixes 73 vulnerabilities in June 2021 Platform Update
- Google Patches Critical Android RCE Bug
- Android malware hides as a system update app to spy on you
- Linux system service bug lets you get root on most modern distros

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. A new zero-day Bug in Chrome

Description	
Google Chrome browser for Windows, Mac and Linux are found to be vulnerable to a new zero-day flaw. the internet service company has stated that the chrome browser is addressed to about 14 newly discovered security issues that include a zero-day flaw. It has also been stated that the vulnerability has been exploited in the wild. The vulnerability arises in the browser from the confusion issue in the open-source V8 and JavaScript engine. The technical detail about the exploitation is yet to be disclosed however, Google's Threat Analysis Group hints that the threat actors that have exploited this vulnerability are the same who exploited remote code execution flaw in the Microsoft Windows MSHTML platform.	
Source	https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop.html
Infected Technology	Google Chrome
CVE ID	CVE-2021-30551
Recommendation	Update Google Chrome to the latest version (91.0.4471.101)

2. Samsung pre-installed apps are exploited for spying

Description	
The pre-installed apps in Samsung mobiles devices are at the risk of multiple vulnerabilities. The vulnerabilities within these applications could be exploited to spy over the victim and also be leveraged to take full control of the device. This information has been released as a result of a bug bounty program conducted to identify the vulnerabilities. The identified vulnerabilities could enable attackers to steal SMS messages by tricking the victim and read/write arbitrary files with elevated permissions without requiring user interaction. The reading and writing capability on the vulnerable device allows threat actors to access the contact list, information in the SD card which could ultimately lead to the disclosure of personal information such as phone number, address, photos, and email addresses.	
Source	https://blog.oversecured.com/Two-weeks-of-securing-Samsung-devices-Part-1/
Infected Technology	Samsung Mobile Devices
Recommendation	Install the latest firm updates released by Samsung

3. Dual vulnerability combo in popular CMS Joomla could lead to ‘full system compromise’	
Description	
A fix has been released for one flaw, but Joomla maintainers are disputing the severity of a second fault. According to the report if the two vulnerabilities are chained together, the adversaries could achieve full system compromise. When the password reset vulnerability and the stored XSS issue are coupled, the attacker may be able to get control of the website and upload a PHP shell that allows them to run commands on the server. An attacker can reset an administrator's password using the password reset vulnerability then uses stored XSS vulnerability, to target the ‘Super Admin' user. By gaining ‘Super Admin’ access, an attacker can execute a remote code execution (RCE) attack.	
Source	https://www.fortbridge.co.uk/advisories/joomla-password-reset-vulnerability-and-stored-xss-for-full-compromise/
Infected Technology	Joomla Content Management System (CMS)
Recommendation	Apply the patch as soon as possible

4. Microsoft patches six Windows zero-days, including a commercial exploit	
Description	
Microsoft has fixed 50 vulnerabilities, including six actively exploited Windows zero-days, in what is the company's largest batch of actively exploited zero-days ever patched in one go. Details about how the six zero-days have been kept under wraps, as is usually the case with these types of disclosures, primarily to give defenders more time to apply patches before other threat actors can learn how to exploit the bugs. Microsoft has fixed problems including remote code execution (RCE) bugs, denial-of-service issues, privilege escalation, and memory corruption issues.	
Source	https://therecord.media/microsoft-patches-six-windows-zero-days-including-a-commercial-exploit/?web_view=true
Infected Technology	Microsoft Windows
CVE ID	CVE-2021-33742, CVE-2021-31955, CVE-2021-31956, CVE-2021-31962, CVE-2021-31199, CVE-2021-31201
Recommendation	Update the system to latest version

5. Adobe Patches Major Security Flaws in PDF Reader, Photoshop

Description	
Adobe has released security updates for Adobe Acrobat and Reader for Windows and macOS. These updates address multiple critical vulnerabilities. The most serious of the vulnerabilities could allow attackers to take complete control of a Windows or macOS machine with minimal user action. In some cases, malicious exploits can be triggered remotely to hijack unpatched machines. Adobe also issued a separate bulletin to document a pair of potentially dangerous buffer overflow flaws in Adobe Photoshop that expose both Windows and macOS users to code execution attacks.	
Source	https://helpx.adobe.com/security/products/acrobat/apsb21-37.html
Infected Technology	Adobe Acrobat and Reader, Adobe Photoshop
Recommendation	Update the products to the latest versions

6. Microsoft Office MSGraph vulnerability could lead to code execution

Description	
Microsoft today will release a patch for a vulnerability affecting the Microsoft Office MSGraph component, responsible for displaying graphics and charts, that could be exploited to execute code on target machine. Because the component can be embedded in most Office documents, an attacker can use it to deliver a malicious payload without the need for special functions. This type of flaw consists of incorrect use of dynamic memory during program operation and can lead to arbitrary code execution on the system. According to the researchers, the issue is in a MSGraph file parsing function, which is commonly used across multiple different Microsoft Office Products.	
Source	https://research.checkpoint.com/2021/fuzzing-the-office-ecosystem/
Infected Technology	Microsoft Excel (EXCEL.EXE), Office Online Server (EXEELCNV.EXE), and Excel for OSX.
CVE ID	CVE-2021-31939
Recommendation	Consider upgrading Microsoft to the latest patched version.

7. Intel fixes 73 vulnerabilities in June 2021 Platform Update

Description	
Intel has addressed 73 security vulnerabilities as part of the June 2021 Patch Tuesday, including high severity ones impacting some versions of Intel's Security Library and the BIOS firmware for Intel processors. In the security updates, Intel addressed five high severity vulnerabilities of which the first one is caused by incomplete cleanup in some Intel VT-d products that could enable authenticated attackers to escalate privileges via local access. Similarly, Intel also patched four more bugs caused by improper initialization, race condition, improper input validation, and insufficient control flow management in the CPU BIOS firmware allowing escalation of privilege via local or physical access.	
Source	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24489
Infected Technology	Intel Security Library and BIOS firmware (Intel Processors)
CVE ID	CVE-2021-24489, CVE-2020-12357, CVE-2020-8670, CVE-2020-8700, CVE-2020-12359
Recommendation	Consider applying the released patch.

8. Google Patches Critical Android RCE Bug

Description	
Google patched more than 90 security vulnerabilities in its Android operating system impacting its pixel devices and third-party Android handsets, including a critical remote code-execution bug that could allow an attacker to commandeer a targeted vulnerable mobile device. According to the Google's June security bulletin, that bug exists in the System component in the Android OS and could enable a remote attacker using a specially crafted transmission to execute arbitrary code within the context of a privileged process. It's the most severe bug of those patched so far this June, the company said.	
Source	https://source.android.com/security/bulletin/2021-06-01
Infected Technology	Android Operating System
CVE IDs	CVE-2021-0507
Recommendation	Consider applying the security patches released by google.

9. Android malware hides as a system update app to spy on you

Description	
A new, "sophisticated" Android spyware app disguising itself as a software update has been discovered by researchers. According to Zimperium zLabs, the malware masquerades as a System Update application while quietly exfiltrating user and handset data. It should be noted that the sample app detected by the team was found on a third-party repository and not the official Google Play Store. Once installed, the victim's device is registered with a Firebase command-and-control (C2) server used to issue commands while a separate, dedicated C2 is used to manage data theft. The malware is a Remote Access Trojan (RAT) and able to steal GPS data and SMS messages, contact lists, call logs, harvest images and video files along with various additional sensitive information.	
Source	https://blog.zimperium.com/new-advanced-android-malware-posing-as-system-update/
Infected Technology	Android Operating System
Recommendation	Consider verifying the authenticity of the application before downloading it from play store.

10. Linux system service bug lets you get root on most modern distros

Description

Unprivileged attackers can get a root shell by exploiting an authentication bypass vulnerability in the polkit auth system service installed by default on many modern Linux distributions. Exploiting this vulnerability is surprisingly easy as it only takes a few terminal commands using only one standard tool such as bash, kill, and dbus-send. Red Hats’ security advisory explains that when a requesting process disconnects from dbus-daemon just before the call to polkit_system_bus_name_get_creds_sybc starts, the process cannot get a unique uid and pid of the process and it cannot verify the privileges of the requesting process. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

Source	https://access.redhat.com/security/cve/CVE-2021-3560
Infected Technology	RHEL 8, Fedora 21 (or later), Ubuntu 20.04, Debian testing (‘bullseye’)
CVE ID	CVE-2021-3560
Recommendation	Mitigation of this issue is currently not available. However, consider upgrading to the patched version as soon as it is available.

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