March 15, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Critical Pre-Auth RCE Flaw Found in F5 Big-IP Platform – Patch ASAP
- Another Google Chrome 0-Day Bug Found Actively Exploited In-the-Wild
- Apple Issues Patch for Remote Hacking Bug Affecting Billions of its Devices
- Microsoft Issues Security Patches for 89 Flaws — IE 0-Day Under Active Attacks
- Samsung fixes critical Android bugs in March 2021 updates
- Vulnerability That Allows Complete WordPress Site Takeover Exploited in the Wild
- SAP Patches Critical Flaws in MII, NetWeaver Products

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. Critical Pre-Auth RCE Flaw Found in F5 Big-IP Platform – Patch ASAP

Description	
On Wednesday Application security company F5 Networks published an advisory warning of four critical vulnerabilities impacting multiple products that could result in denial of service (DoS) attacks and even unauthenticated remote code execution on target networks. Successful exploitation of these vulnerabilities could lead to a full compromise of vulnerable systems, including the possibility of remote code execution as well as trigger a buffer overflow, leading to a DoS attack. According to F5 Network, the vulnerabilities were discovered as a result of regular and continuous internal security testing of their solutions. Alongside, F5 Network urges their customers to update their BIG-IP and BIG-IQ deployments to a fixed version as soon as possible.	
Source	https://support.f5.com/csp/article/K02566623 https://www.f5.com/company/blog/big-ip-and-big-iq-vulnerabilities-protecting-your-organization
Infected Technology	BIG-IP versions: 16.0.1.1, 15.1.2.1, 14.1.4, 13.1.3.6, 12.1.5.3, and 11.6.5.3 BIG-IQ versions: 8.0.0, 7.1.0.3, and 7.0.0.2
CVE ID	CVE-2021-22986, CVE-2021-22987, CVE-2021-22988, CVE-2021-22989, CVE-2021-22990, CVE-2021-22991, CVE-2021-22992
Recommendation	Consider updating BIG-IP and BIG-IQ deployments to a fixed version.

2. Another Google Chrome 0-Day Bug Found Actively Exploited In-the-Wild

Description	
Google has addressed yet another actively exploited zero-day in Chrome browser, marking the second such fix released by the company within a month. The browser maker on Friday shipped 89.0.4389.90 for Windows, Mac, and Linux, which is expected to be rolling out over the coming days/weeks to all users. While the update contains a total of five security fixes, the most important flaw rectified by Google concerns the use after free vulnerability in its Blink rendering engine. With this update, Google has fixed three zero-day flaws in Chrome since the start of the year. Chrome users can update to the latest version of Google Chrome to mitigate the risk associated with the flaw.	
Source	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_12.html
Infected Technology	Google Chrome
CVE-ID	CVE-2021-21191, CVE-2021-21192, CVE-2021-21193
Recommendation	Consider updating Google Chrome to its latest version.

3. Apple Issues Patch for Remote Hacking Bug Affecting Billions of its Devices

Description	
Apple has released out-of-band patches for ios, macOS, watchOS, and Safari web browsers to address a security flaw that could allow attackers to run arbitrary code on devices via malicious web content. According to the update notes posted by Apple, the flaw stems from a memory corruption issue that could lead to arbitrary code execution when processing specially crafted web content. However, the update is now available for devices running ios 14.4, iPadOS 14.4, macOS Big Sur, and watchOS 7.3.1, and as an update to Safari for MacBooks running macOS Catalina and macOS Mojave.	
Source	https://support.apple.com/en-us/HT212221 https://support.apple.com/en-us/HT212220 https://support.apple.com/en-us/HT212222 https://support.apple.com/en-us/HT212223
Infected Technology	iOS < 14.4, iPadOS <14.4, watchOS < 7.3.1, macOS Big Sur, Safari
CVE ID	CVE-2021-1844, CVE-2021-1782, CVE-2021-1870, CVE-2021-1871
Recommendation	Consider applying the security patches provided by Apple.

4. Microsoft Issues Security Patches for 89 Flaws — IE 0-Day Under Active Attacks

Description
Microsoft released patches for 89 flaws including fixes for an actively exploited zero-day in Internet Explorer that could permit an attacker to run arbitrary code on target machines. Of these flaws, 14 are listed as Critical, and 75 are listed as Important in severity, out of which two of the bugs are described as publicly known, while five others have been reported as under active attack at the time of release. Among those five security issues is a clutch of vulnerabilities known as Proxy Logon that allows adversaries to break into Microsoft Exchange Servers in target environments and subsequently allow the installation of unauthorized web-based backdoors to facilitate long-term access. Aside from these actively exploited vulnerabilities, the update also corrects several remote code execution (RCE) flaws in Windows DNS Server, Hyper-V Server, SharePoint Server, and Azure Sphere.

Source	https://msrc.microsoft.com/update-guide/releaseNote/2021-Mar
Infected Technology	Microsoft Products
CVE-ID	CVE-2021-1640, CVE-2021-24089, CVE-2021-24104, CVE-2021-24107, CVE-2021-24108, CVE-2021-24110, CVE-2021-26411, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-26859, CVE-2021-26867, CVE-2021-26869, CVE-2021-26877, CVE-2021-26884, CVE-2021-26887, CVE-2021-26893
Recommendation	Consider installing the security updates provided by Microsoft.

5. Samsung fixes critical Android bugs in March 2021 updates

Description

This week Samsung started rolling out Android's March security updates to mobile devices to patch critical security vulnerabilities in the runtime, operating system, and related components. This comes after Android had published their March 2021 security updates bulletin, which includes patches for critical vulnerabilities impacting the latest devices. These updates mainly comprise significant security fixes with a couple of enhancements across Samsung Galaxy built-in apps. Every vulnerability addressed by this update, has either a 'High' or 'Critical' severity rating, making this update a must for Android users so that their devices remain protected. As put by Android advisory, among the several vulnerabilities, flaws impacting components like Framework, System, and Android runtime could allow sensitive information disclosure and privilege escalation by attackers.

Source	https://doc.samsungmobile.com/SM-G977B/EVR/doc.html
Infected Technology	Android Devices (Samsung)
CVE ID	CVE-2021-0395, CVE-2021-0391, CVE-2021-0398, CVE-2021-0397, CVE-2017-14491, CVE-2021-0393, CVE-2021-0396, CVE-2021-0390, CVE-2021-0392, CVE-2021-0394, CVE-2021-0390
Recommendation	• Consider updating Samsung devices to the latest patched versions.

6. Vulnerability That Allows Complete WordPress Site Takeover Exploited in the Wild

Description

A critical vulnerability identified in The Plus Addons for Elementor WordPress plugin could be exploited to gain administrative privileges to a website. The zero-day has been exploited in the wild, the Wordfence team at WordPress security company Defiant warns. With more than 30,000 installations to date, The Plus Addons for Elementor is a premium plugin that has been designed to add several widgets to be used with the popular WordPress website builder Elementor. The identified issue, Wordfence explains, resides in one of the added widgets, which provides the ability to insert user login and registration forms to Elementor pages. Because the functionality is not properly configured, an attacker can create a new administrative user account on the vulnerable site, or even log in as an existing administrative user, the researchers reveal.

Source	https://www.wordfence.com/blog/2021/03/critical-0-day-in-the-plus-addons-for-elementor-allows-site-takeover/
Infected Technology	The Plus Addons
CVE ID	CVE-2021-24175
Recommendation	Consider using plugins alternative to The Plus Addons.

7. SAP Patches Critical Flaws in MII, NetWeaver Products

Description	
SAP has released 18 new and updated SAP Security Notes in its March 2021 patch release, including the notes that were released since the last patch day. The patches include critical vulnerabilities affecting the company's NetWeaver Application Server (AS) and Manufacturing Integration and Intelligence (MII) products. This month's set of patches also includes 4 updates to previously released Patch Day security notes, including updates for two notes rated Hot News (CVSS score 10), which address a missing authorization check in Solution Manager and deliver the latest patches for the Chromium browser in Business Client. The most severe of the newly released security notes address a code injection vulnerability in SAP MII, the vulnerability features a CVSS score of 9.9.	
Source	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=571343107
Infected Technology	MII, NetWeaver Products
CVE-ID	CVE-2020-6207, CVE-2021-21480, CVE-2021-21481, CVE-2021-21484
Recommendation	Update the corresponding technologies with the released patches.

8. Microsoft Exchange Servers are targeted with ransomware

Description	
Cybersecurity experts have warned that an unpatched Exchange Server software could open a pathway for ransomware infection in an extension to swift escalation procedure. In recent reports, the malicious attackers have been leveraging the heavily exploited ProxyLogon. It is an Exchange Server flaw that allows the installation of the new strain of ransomware typically called "DearCry". DearCry referred to as 'copy ransomware', creates an encrypted copy of attacker files with the use of encryption keys that is embedded within the ransomware binary and deletes the user data and the original version of software hence, allowing the retrieval of some data. The successful weaponization could lead enable threat actors to gain persistent system access and control of an enterprise network hence, risking potential data theft, file encryption and preventing access to the organization's mailboxes.	
Source	https://twitter.com/MsftSecIntel/status/1370236539427459076
Infected Technology	Microsoft Exchange Server

9. Unpatched Flaws in Netgear Business Switches Expose Organizations to Attacks

Description

Multiple vulnerabilities are found in ProSAFE Plus JGS516PE and GS116Ev2 business switches from Netgear, the most severe of which could allow a remote, unauthenticated attacker to execute arbitrary code. A total of 15 vulnerabilities affecting Netgear switches that use the ProSAFE Plus configuration utility were found to expose users to various risks, according to researchers with IT security firm NCC Group. The most important of these bugs is, an unauthenticated remote code execution flaw rated critical severity (CVSS score of 9.8). Affecting firmware versions prior to 2.6.0.43, the bug is related to the internal management web application not implementing the correct access controls, which could allow attackers to bypass authentication and run code with the privileges of the administrator.

Source	https://research.nccgroup.com/2021/03/08/technical-advisory-multiple-vulnerabilities-in-netgear-prosafe-plus-jgs516pe-gs116ev2-switches/
Infected Technology	ProSAFE Plus JGS516PE and GS116Ev2 business switches
CVE ID	CVE-2020-26919, CVE-2020-35231, CVE-2020-35220, CVE-2020-35232, CVE-2020-35224, CVE-2020-35221, CVE-2020-35229, CVE-2020-35228, CVE-2020-35227, CVE-2020-35226, CVE-2020-35222, CVE-2020-35233, CVE-2020-35225, CVE-2020-35230, CVE-2020-35223
Recommendation	Consider Updating to firmware version 2.6.0.48

10. A browser attack allows tracking of users online with JavaScript disabled

Description

A new-side channel has been identified that is exploited to leak information from web browsers. The side channel could be leveraged to track users when JavaScript is disabled completely. As the side-channel does not require JavaScript to run, the script blockers are unable to stop it, hence, is extremely difficult to prevent it without modifying deep parts of the operating system. Along with avoiding JavaScript, the side-channel attacks can perform microarchitectural website fingerprinting attacks in various hardware platforms such as Intel Core, AMD Ryzen, Samsung Exynos, and Apple M1 CPUs. The side-channel attacks work on indirect data gatherings such as timing, sound, power consumption, vibrations, and electromagnetic emissions. The exploits of side-channel target the shared use of a processor's component, leading to the disclosure of secret information of cryptographic keys.

Source	https://arxiv.org/abs/2103.04952
Infected Technology	Web Browsers

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/