April 19
2021

INFOSEC WEEKLY

#MADE4SECURITY

- Update Your Chrome Browser to Patch Two New In-the-Wild 0-day Exploits
- WhatsApp flaw lets anyone lock you out of your account
- Exploit Released for Critical Vulnerability Affecting QNAP NAS Devices
- Critical RCE can allow attackers to compromise Juniper Network devices
- Linux, macOS malware hidden in fake NPM package
- Another Critical Vulnerability Patched in SAP Commerce
- Adobe Patches Critical Code Execution Vulnerabilities in Photoshop, Bridge

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. Update Your Chrome Browser to Patch Two New In-the-Wild 0-day Exploits

Description

Google on Tuesday released a new version of Chrome web-browsing software for Windows, Mac, and Linux with patches for two newly discovered security vulnerabilities for both of which are exploits that allow attackers to engage in active exploitation. One of the two flaws exists due to insufficient validation of untrusted input in its V8 JavaScript rendering engine, which Google had already fixed but security researcher Rajvardhan Agrawal has published a working exploit by reverse-engineering the patch that the Chromium team pushed to the open-source component. According to him, there is one more vulnerability affecting Chromium-based browsers that have already been patched in the latest version of V8, but has not been included in the Chrome release, thereby leaving users potentially vulnerable to RCE (Remote Code Execution).

Source	https://chromereleases.googleblog.com/
Infected Technology	Chrome Browser
CVE ID	CVE-2021-21220, CVE-2021-21206
Recommendation	Consider updating Chrome as soon as the latest version: Chrome 89.0.4389.128 gets released.

2. WhatsApp flaw lets anyone lock you out of your account

Description

A flaw in WhatsApp could allow an attacker to lock any victim out of the app using just their phone number and without requiring any action on their part. The underlying loophole abuses a lapse in security of two independent WhatsApp processes. In general, we use our number to confirm our identity, but if hackers were to use that number and WhatsApp sent the verification code repeatedly and if We disregarded it, then the requests would trigger WhatsApp's limit on the number of times the codes can be sent and would also cause codes to be blocked after several wrong attempts – both for 12 hours. Then, they would create a new email address and shoot an email to WhatsApp's support with the subject "lost/stolen phone" and will ask them to deactivate the number.

Source	https://www.welivesecurity.com/2021/04/13/whatsapp-flaw-lets-anyone-lock-you-out-account/?&web_view=true
Infected Technology	WhatsApp
Recommendation	Pay attention to the notification and messages you receive and act instantly to any suspicious activities.

3. Exploit Released for Critical Vulnerability Affecting QNAP NAS Devices

Description

An exploit is now publicly available for a remote code execution vulnerability affecting QNAP network-attached storage (NAS) devices that run the Surveillance Station video management system. The security hole is a stack-based buffer overflow that could be abused by remote attackers to execute code on an affected system, without authentication. The issue resides in the insecure use of user-supplied data. An attacker could send a specially crafted HTTP request to a vulnerable QNAP NAS device, which would overflow an internal buffer that the Surveillance Station plugin uses, thus achieving arbitrary code execution.

Source	https://www.qnap.com/zh-tw/security-advisory/qsa-21-07
Infected Technology	QNAP NAS Surveillance Station versions: 5.1.5.4.2 and 5.1.5.3.2
CVE ID	CVE-2020-2501
Recommendation	Consider updating to the newest patched versions: • Version 5.1.5.4.3 for 64-bit ARM CPU NAS • Version 5.1.5.3.3 for 32-bit ARM CPU NAS and x86 CPU NAS

4. Critical RCE can allow attackers to compromise Juniper Network devices

Description

Cybersecurity vendor Juniper Networks addressed a critical vulnerability in Junos OS that could allow an attacker to remotely hijack or disrupt affected devices. This flaw stems from the improper buffer size validation, which can lead to a buffer overflow. The flaw can be exploited by a remote, unauthenticated attacker to execute arbitrary code of a vulnerable device or to trigger a DoS condition. The vulnerability can be exploited by sending specially crafted packets to the targeted system. An attacker could trigger the flaw to install a backdoor on a vulnerable device or to change its configuration. Juniper SIRT revealed that it is not aware of any attacks in the wild exploiting the above flaw.

Source	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11147
Infected Technology	Junos OS Version 15.1 X 49, 15.1, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.3, 19.4, 20.1, 20.2, and 20.3
CVE ID	CVE-2021-0254
Recommendation	Consider applying the patch released by Juniper.

5. Linux, macOS malware hidden in fake NPM package

Description

A malicious package has been identified in the npm registry that targets the Linux and Apple macOS-based NodeJS developers. The malicious package is called ‘web-browserify’. This package imitates the popular Browserify npm component that has been downloaded 160 million times. The malware is used to execute advanced reconnaissance and fingerprinting processes. The malware uses another legitimate npm component called ‘systeminformation’ to collect a variety of information from the infected system. The collection of information includes system username, docker image information, OS information, Bluetooth-connected devices, Virtual Machine information, CPU information, RAM, and hardware information. The fingerprinting is possible by exfiltrating to an attacker-controlled domain as a plaintext HTTP GET connection.

Source	https://blog.sonatype.com/damaging-linux-mac-malware-bundled-within-browserify-npm-brandjack-attempt
Infected Technology	Linux and macOS
Recommendation	Consider removing the web-browserify npm package immediately.

6. Another Critical Vulnerability Patched in SAP Commerce

Description

On Tuesday, as part of its April 2021 Security Patch Day, SAP announced the release of 14 new security notes and 5 updates to previously released notes. The only new Hot News note released with this round of patches addresses a critical vulnerability in SAP Commerce. According to SAP, the critical security hole could be abused to achieve remote code execution with a critical impact on the system’s confidentiality, integrity, and availability. The issue allows authorized users of SAP Commerce Backoffice software to inject malicious code in source rules by abusing the scripting capabilities of the Rules engine. To address the vulnerability, SAP has introduced additional validations and output encoding when processing rules.

Source	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649
Infected Technology	SAP Commerce
CVE ID	CVE-2021-27602
Recommendation	Consider applying the security patches released by SAP.

7. Adobe Patches Critical Code Execution Vulnerabilities in Photoshop, Bridge

Description

Adobe patches vulnerabilities in four of its products, including critical code execution flaws affecting Photoshop and Bridge. In Photoshop, the company fixed two critical buffer overflow bugs that can be exploited for arbitrary code execution in the context of the targeted user. In its Bridge asset management software, Adobe resolved four critical vulnerabilities that can lead to code execution, including two memory corruption issues and two out-of-bounds write issues. The latest Bridge updates also fix a couple of important-severity information disclosure and privilege escalation vulnerabilities.

Source	https://www.securityweek.com/adobe-patches-critical-code-execution-vulnerabilities-photoshop-bridge?&web_view=true
Infected Technology	Adobe Photoshop and Adobe Bridge
CVE ID	CVE-2021-28548, CVE-2021-28549, CVE-2021-21091, CVE-2021-21096, CVE-2021-21093, CVE-2021-21092, CVE-2021-21094, CVE-2021-21095
Recommendation	Update the Software to the latest version

8. 1-Click hack identified in popular Desktop apps

Description

Various one-click vulnerabilities have been revealed across popular software applications predominantly desktop-based. These vulnerabilities allow the attacker to execute potential arbitrary code on the target system or endpoint. The issues were identified by Positive Security researchers in which they assert that the flaws originate from an insufficient validation of URL input. The URL input opened with the underlying operating system leads to the inadvertent execution of a malicious file. The researchers also identified that the applications were not able to validate the URL hence, allowing a malicious attacker to craft specific links pointing to a piece of attack code that ultimately lead to remote code execution.

Source	https://positive.security/blog/url-open-rce
Infected Technology	Nextcloud, Telegram, VLC Player, OpenOffice, LibreOffice, Mumble, Dogecoin, Bitcoin ABC, Bitcoin Cash, Wireshark, WinSCP
CVE ID	CVE-2021-22879, CVE-2021-30245, CVE-2021-25631, CVE-2021-27229, CVE-2021-22191, CVE-2021-3331

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/