February 08, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- New Chrome Browser 0-day Under Active Attack
- Recent root-giving Sudo bug also impacts macOS
- SonicWall issues firmware patch after attackers exploited critical bugs
- Three new security vulnerabilities found in SolarWinds
- Cisco fixes critical code execution bugs in SMB VPN routers
- Weak ACLs in Adobe ColdFusion Allow Privilege Escalation
- Chrome extensions are caught hijacking Google Search results
- Apple Issues Patches for NAT Slipstreaming 2.0 Attack
- Google Patches Over a Dozen High-Severity Privilege Escalation Flaws in Android

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. New Chrome Browser 0-day Under Active Attack

Description

Google has patched a zero-day vulnerability in Chrome web browser for desktop that it says is being actively exploited in the wild. The company released 88.0.4324.150 for Windows, Mac, and Linux, with a fix for a heap buffer overflow flaw in its V8 JavaScript rendering engine. According to Google, the attack was carried out by North Korean hackers against security researchers with an elaborate social engineering campaign to install a Window backdoor. Some researchers were infected simply by visiting a fake research blog on fully patched systems running Windows 10 and Chrome browser.

Source	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_4.html
Infected Technology	Google Chrome
CVE-ID	CVE-2021-21148
Recommendation	Update Google Chrome to its latest version.

2. Recent root-giving sudo bug also impacts macOS

Description

The vulnerability, disclosed by security researchers from Qualys, impacted Sudo, an app that allows admins to delegate limited root access to other users. This bug in the Sudo app can let attackers with access to a local system elevate their access to a root-level account. Previously only UNIX-based systems like Debian, Ubuntu, fedora, etc. were identified to be affected by the vulnerability, however, Matthew Hickey, the co-founder of Hacker House, pointed out that the recent version of macOS also ships with the sudo. Upon verification CVE-2021-3156 vulnerability with a few modifications could be used to grant attackers access to macOS root accounts as well. The findings were also privately and independently verified and confirmed to ZDNet by Patrick Wardle, one of today's leading macOS security experts, and publicly by Will Dormann, a vulnerability analyst at the Carnegie Mellon University's CERT Coordination Center.

Source	https://www.zdnet.com/article/recent-root-giving-sudo-bug-also-impacts-macos/?&web_view=true
Infected Technology	macOS
Recommendation	Update sudo to the latest version

3. SonicWall issues firmware patch after attackers exploited critical bugs

Description	
SonicWall has released a critical patch for two vulnerabilities in its Secure Mobile Access 100 series products featuring 10.x firmware, which malicious actors exploited in a cyberattack against the infosec firm last month. One flaw consists of an exploit that enables admin credentials access, and the other is a remote code execution attack. A SonicWall security advisory describes one vulnerability as a SQL injection bug in the SonicWall SSLVPN SMA100 product that allows a remote unauthenticated attacker to perform SQL query to access username, password, and other session-related information.	
Source	https://www.sonicwall.com/support/product-notification/urgent-patch-available-for-sma-100-series-10-x-firmware-zero-day-vulnerability-updated-feb-3-2-p-m-cst/210122173415410/
Infected Technology	Physical and Virtual SMA 100 10.x devices SMA 200, SMA 210, SMA 400, SMA 410, SMA500v
Recommendation	Install the SonicWall patch on the affected SMA 100 series 10.x code.

4. Weak ACLs in Adobe ColdFusion Allow Privilege Escalation

Description	
This week, Will Dormann, a security researcher with Carnegie Mellon University's CERT Coordination Center (CERT/CC), revealed that the Adobe ColdFusion installer does not create a secure access-control list (ACL) on the default installation directory. Due to the lack of properly set ACL, any unprivileged user could create files in the platform's directory structure, which leads to a privilege escalation security flow. An unprivileged user on a Windows computer could place a specially crafted DLL file within the installation directory of Adobe ColdFusion, which would result in arbitrary code being executed with SYSTEM privileges resulting in what is known to be DLL hijacking.	
Source	https://kb.cert.org/vuls/id/125331
Infected Technology	ColdFusion 2016, 2018, 2021
Recommendation	Consider using ColdFusion Server Auto-Lockdown installer

5. Three new security vulnerabilities found in SolarWinds

Description
According to Trustwave, SolarWinds Orion Platform was found vulnerable to two flaws and the Serv-U FTP server for Windows was found with a separate weakness flaw. These security issues had not been exploited during the supply chain attack that had targeted Orion Platform of December 2020. The first flaw in Orion Platform allowed unauthenticated attackers to send messages to queues over TCP port 1801 eventually attaining RCE by chaining it with another unsafe deserialized issue in the code handling the incoming message. The second Orion flaw lets unprivileged users take complete control over the backend database hence, stealing information and adding admin-level users inside Orion Products. The flaw in SolarWinds Serv-U FTP Server for Windows allows an attacker to log into the system locally or remotely to drop file as an admin user with full access to the C:\ drive. The flaw can be leveraged to read and replace the files on the C:\ drive by logging in as an FTP user.

Source	https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/full-system-control-with-new-solarwinds-orion-based-and-serv-u-ftp-vulnerabilities/
Infected Technology	SolarWinds Orion Platform and Serv-U FTP server for Windows
CVE_ID	CVE-2021-25274, CVE-2021-25275, CVE-2021-25276
Recommendation	Consider installing the latest versions of Orion Platform and Serv-U FTP (15.2.2 Hotfix 1)

6. Zero-day vulnerabilities in WordPress Plugin

Description
Researchers from TIM's Red Team Research (RTR) discovered 2 new zero-day vulnerabilities in WordPress Plugin Limit Login Attempts Reloaded. A rate-limiting bypass under a non-default configuration, which effectively defeats the plugin's purpose to prevent the brute force attack and an unauthenticated reflected XSS. The first one, Improper Restriction of Excessive Authentication Attempts (CWE-307) has a CVSS3 score of 9.8. The second one, Improper Neutralization of Input During Web Page Generation (CWE-79) has a CVSS3 score of 5.4.

Source	https://securityaffairs.co/wordpress/114186/hacking/zero-day-wordpress.html?web_view=true
Infected Technology	Websites using WordPress
CVE_ID	CVE-2020-35589, CVE-2020-35590
Recommendation	Update the plugins to the latest version.

7. Hugely Popular 'The Great Suspender' Chrome Extension Contains Malware

Description	
Google on Thursday removed the "The Great Suspender", a popular chrome extension used by millions of users, from its Chrome Web Store for containing malware. The add-on is alleged to have stealthily added features that could be exploited to execute arbitrary code from a remote server, including tracking users online and committing advertising fraud. The extension, which had more than two million installs before it was disabled, would suspend tabs that aren't in use, replacing them with a blank gray screen until they were reloaded upon returning to the tabs in question. The extension has been said to be sold by the original developer after which the shady behavior has been going around. Microsoft had also blocked the extension in last November.	
Source	https://thehackernews.com/2021/02/warning-hugely-popular-great-suspender.html
Infected Technology	Google Chrome
Recommendation	Remove the extension, if used.

8. Cisco fixes critical code execution bugs in SMB VPN routers

Description	
Cisco has addressed multiple pre-auth remote code execution (RCE) vulnerabilities affecting several small business VPN routers and allowing attackers to execute arbitrary code as root on successfully exploited devices. The security bugs with a severity rating of 9.8/10 were found in the web-based management interface of Cisco small business routers. According to Cisco, these vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf
Infected Technology	Cisco Routers running firmware version < 1.0.01.02, which includes: • RV160 VPN Router • RV160W Wireless-AC VPN Router • RV260 VPN Router • RV260P VPN Router with POE • RV260W Wireless-AC VPN Router
Recommendation	Consider updating the firmware of these routers to the latest release.

9. Apple Issues Patches for NAT Slipstreaming 2.0 Attack

Description

Apple this week released security updates to address multiple vulnerabilities in macOS and Safari, including a flaw that can be exploited for the recently disclosed NAT Slipstreaming 2.0 attack. As part of the attack, an adversary could set up a crafted website and lure the intended victim into visiting it. As soon as that happens, malicious code on the site starts sending multiple fetch requests from the victim's browser, allowing the attacker to identify and access devices on the local network. The attacks bypass Network Address Translation (NAT) and firewalls by abusing the browser and the Application Level Gateway (ALG), a connection tracking mechanism in firewalls, NATs, and routers.

Source	https://support.apple.com/en-gb/HT212147
CVE_ID	CVE-2021-1799
Infected Technology	macOS and Safari
Recommendation	Consider applying the patch provided by Apple.

10. Microsoft office 365 Attacks Sparked from Google Firebase

Description

Researchers said A phishing campaign bent on stealing Microsoft login credentials is using Google Firebase to bypass email security measures in Microsoft Office 365. Researchers at Armorblox uncovered invoice-themed emails sent to at least 20,000 mailboxes that purport to share information about an electronic funds transfer (EFT) payment. The emails carry a fairly vanilla subject line, "TRANSFER OF PAYMENT NOTICE FOR INVOICE," and contain a link to download an "invoice" from the cloud. Clicking that link begins a series of redirects that eventually takes targets to a page with Microsoft Office branding that's hosted on Google Firebase. That page is of course a phishing page bent on harvesting Microsoft log-in information, secondary email addresses, and phone numbers.

Source	https://threatpost.com/microsoft-office-365-attacks-google-firebase/163666/
Infected Technology	Microsoft Office 365
Recommendation	Consider implementing 2FA.

11. Chrome extensions are caught hijacking Google Search results

Description

Avast has found 28 browser extensions that were part of a vast network of rogue extensions. The extensions collectively called “CacheFlow” were found to hijack clicks to link the search results pages to arbitrary URLs that include phishing sites and ads. The rogue extensions include Video Downloader for Facebook, Instagram Story Downloader, Vimeo Video Downloader. The extensions leverage the cache-control HTTP header as a covert channel for retrieving commands from a command-control server controlled by the attacker. The covert channel was used to hide the command-and-control traffic in the analytics request using cache-control HTTP headers. The installed JavaScript-based payload extracts personal information such as birthdates, geolocation, device activity, and email addresses focusing on the data collection from Google.

Source	https://decoded.avast.io/janvojtesek/backdoored-browser-extensions-hid-malicious-traffic-in-analytics-requests/
Infected Technology	Google Chrome and Microsoft Edge
Recommendation	Delete and avoid using unnecessary plugins

12. Google Patches Over a Dozen High-Severity Privilege Escalation Flaws in Android

Description

Google this week published its Android Security Bulletin for February 2021, which includes information on more than 40 vulnerabilities, most of which could lead to elevation of privilege. The most important of these vulnerabilities is a critical flaw in the Media Framework component that allows an attacker to execute arbitrary code on a vulnerable device. The attacker needs to supply a specially crafted file to trigger the bug. According to Google’s Advisory, the issue is considered critical on Android 8.1 and 9 platform releases but has only a high severity rating on Android 10 and 11.

Source	https://source.android.com/security/bulletin/2021-02-01
Infected Technology	Android 8.1, 9, 10, 11
CVE -ID	CVE-2021-0325, CVE-2021-0332, CVE-2021-0335
Recommendation	Apply the security updates once released by device manufacturer

13. Major Vulnerabilities discovered and patched in Realtek RTL8159A Wi-Fi Module

Description	
Researchers from Israeli IoT security firm Vdoo discovered and responsibly disclosed six major vulnerabilities in Realtek's RTL8195A Wi-Fi module. An attacker can gain remote root access to the Wi-Fi module, and from there very possibly hop to the application process as well. Realtek supplies their own "Ameba" API to be used with the device, which allows any developer to communicate easily via Wi-Fi, HTTP, mDNS, MQTT, and more. As part of the module's Wi-Fi functionality, the module supports the WEP, WPA, and WPA2 authentication modes. In their security assessment, they have discovered that the WPA2 handshake mechanism is vulnerable to various stack overflow and read out-of-bounds issues. They can completely take over the module, without knowing the Wi-Fi network password (PSK) and regardless of whether the module is acting as a Wi-Fi access point or client.	
Source	https://www.vdoo.com/blog/realtek-rtl8195a-vulnerabilities-discovered
Infected Technology	Realtek RTL8195A Wi-Fi Module
Recommendation	Update the versions of the Ameba Use a strong, private WPA2 passphrase

14. Unpatched WordPress Plugin Code-Injection Bug Afflicts 50k Sites

Description	
A security bug in Contact Form 7 Style, could allow for malicious JavaScript injection on victim website in a WordPress plugin installed on over 50,000 sites. The latest WordPress plugin security vulnerability is a cross-site request forgery (CSRF) to stored cross-site scripting (XSS) problem in Contact Form 7 Style, which is an add-on to the well-known Contact Form 7 umbrella plugin. CSRF allows an attacker to induce a victim user to perform actions that they do not intend to. XSS allows an attacker to execute arbitrary JavaScript within the browser of a victim user. This bug connects the two approaches.	
Source	https://www.wordfence.com/blog/2021/02/unpatched-vulnerability-50000-wp-sites-must-find-alternative-for-contact-form-7-style/
Infected Technology	Contact From 7 Style plugin
Recommendation	Deactivate and Remove the Contact Form & Style plugin

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**