February 15, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Microsoft issues Patches for In-the-Wild 0-day and 55 Others Windows Bug
- Apple fixes SUDO root privilege escalation flaw in macOS
- Critical Firefox Vulnerability Can Allow Code Execution If Chained with Other Bugs
- Internet Explorer 11 zero-day vulnerability gets unofficial micropatch
- Intel patches Tens of Vulnerabilities in Software, Hardware products
- Microsoft patches SharePoint, Excel RCE bugs in Office February security updates
- SAP Commerce Critical Security Bug Allows RCE

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. Microsoft issues Patches for In-the-Wild 0-day and 55 Others Windows Bug

Description	
Microsoft on Tuesday issued fixes for 56 flaws, including a critical vulnerability that's known to be actively exploited in the wild. In all, 11 are listed as Critical, 43 are listed as important, and two are listed as Moderate in severity – six of which are previously disclosed vulnerabilities. The most critical of the flaws in windows Win32k privilege escalation vulnerability that allows attackers with access to a target system to run malicious code with elevated permissions. It could be used to escape the sandbox of Microsoft [Internet Explorer] browser or Adobe reader on the latest Windows 10 version.	
Source	https://msrc.microsoft.com/update-guide/releaseNote/2021-Feb
Infected Technology	Microsoft Products
CVE-ID	CVE-2021-1732, CVE-2021-21017, CVE-2021-24078 CVE-2021-26701, CVE-2021-24081, CVE-2021-1722 CVE-2021-24077, CVE-2021-1472, CVE-2021-24100 CVE-2021- 24074, CVE-2021-24094, CVE-2021-24086
Recommendation	Consider installing the latest security updates provided by Microsoft.

2. Apple fixes SUDO root privilege escalation flaw in macOS

Description	
Apple has rolled out a fix for a critical vulnerability in macOS Big Sur, Catalina, and Mojave that could allow unauthenticated local users to gain root-level privileges on the system. The vulnerability first came to light last month after security auditing firm Qualys disclosed the existence of a heap-based buffer overflow. Although the vulnerability can only be exploited by an attacker already having access to a vulnerable host, the barrier could be easily bypassed by planting malware on a device or brute-forcing a low-privileged service account.	
Source	https://support.apple.com/en-us/HT212177
Infected Technology	macOS
CVE-ID	CVE-2021- 3156
Recommendation	Consider installing the latest security updates provided by Apple.

3. Critical Firefox Vulnerability Can Allow Code Execution if Chained with Other Bugs

Description	
An update released recently by Mozilla for Firefox 85 patches a critical information disclosure vulnerability that can be chained with other security flaws to achieve arbitrary code execution. The bug, as of now, does not have a CVE identifier, however, Mozilla described it as a buffer overflow in-depth pitch calculations for compressed textures. The vulnerability is an information disclosure bug that exists within the implementation of the compressedTexImage 3D API method in WebGL2. Exploitation requires the attacker to convince the targeted user to visit a malicious web page or open a malicious file. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process.	
Source	https://www.mozilla.org/en-US/security/advisories/mfsa2021-06/
Infected Technology	Firefox and Firefox ESR in Windows operating systems.
Recommendation	Consider upgrading to Firefox 85.0.1 and Firefox ESR 78.7.1

4. Internet Explorer 11 zero-day vulnerability gets unofficial micropatch

Description	
An Internet Explorer 11 zero-day vulnerability used against security researchers, received a micropatch that prevents exploitation. At this time, Microsoft has not publicly acknowledged the Internet Explorer zero-day or assigned a CVE identifier to the vulnerability. However, oPatch has announced that they have begun to push out a micropatch for the Internet Explorer 11 vulnerability as it was actively used in the attack. Until Microsoft comes up with an official patch, users can register an account at opatch and install the agent to get access to this micropatch. This patch is free for personal non-profit/educational users.	
Source	https://www.bleepingcomputer.com/news/security/internet-explorer-11-zero-day-vulnerability-gets-unofficial-micropatch/
Infected Technology	Internet Explorer 9, 10, 11
CVE- ID	CVE-2020-0674
Recommendation	Consider applying the security patch provided by Opatch.

5. Intel patches Tens of Vulnerabilities in Software, Hardware products

Description

Intel patches the list of high-severity flaws includes a privilege escalation issue in the Intel Solid State Drive (SSD) Toolbox and a denial-of-service (DoS) flaw in the XMM 7360 Cell Modem that can be exploited by an unauthenticated attacker who has network access. Intel also informed customers about five vulnerabilities in Server Board, Server System and Compute Modules Baseboard Management Controller (BMC) products, including two high-severity privilege escalation issues. Medium-severity vulnerabilities have been patched in RealSense Depth Camera Manager (DCM), Ethernet I210 Controller series network adapters, Trace Analyzer and Collector, SOC Driver Package for STK1A32SC, Ethernet E810 adapter drivers for Linux and Windows, 722 Ethernet controllers, Software Guard Extensions (SGX), Extreme Tuning Utility (XTU), Quartus Prime software, PROSet/Wireless WiFi and Killer drivers for Windows 10, Enhance Privacy ID (EPID) SDK, Server Board Onboard Video driver for Windows, Collaboration Suite for WebRTC, and the Optane DC Persistent Memory installer for Windows.

Source	https://www.intel.com/content/www/us/en/security-center/default.html
Infected Technology	Intel products
Recommendation	Consider applying the patches provided by Intel.

6. SAP Commerce Critical Security Bug Allows RCE

Description

The critical SAP cybersecurity flaw could allow for the compromise of an application used by e-commerce businesses. SAP is warning of a critical vulnerability in its SAP Commerce platform for e-commerce businesses. If exploited, the flaw could allow for remote code execution (RCE) that ultimately could compromise or disrupt the application. The vulnerability assigned CVSS score of 9.9 exists in the system due to misconfiguration of the default user permissions that are shipped with SAP. Consequently, it allows certain users with required privileges to edit Drools rules, which is an engine that makes up the rules engine for SAP Commerce.

Source	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=568460543
Infected Technology	SAP Commerce version 1808, 1811,1905, 2005, and 2011
CVE-ID	CVE-2021-21477
Recommendation	Consider applying the patch released by SAP.

7. Critical Vulnerability fixed in WordPress plugin with 800K installs

Description	
NextGen Gallery, a WordPress plugin used for creating image galleries, has addressed two severe CSRF vulnerabilities to protect sites from potential takeover attacks. Both security vulnerabilities are Cross-Site Request Forgery (CSRF) bugs which can lead to Reflected Cross-Site Scripting (XSS) and remote code execution (RCE) attacks via file upload or Load File Inclusion (LFI). Attackers can exploit these security flaws by tricking WordPress admins into clicking specially crafted links or attachments to execute malicious code in their browsers. Following successful exploitation, the vulnerabilities can let hackers set up malicious redirects, inject spam, abuse compromised sites for phishing, and ultimately, take over the sites completely.	
Source	https://www.wordfence.com/blog/2021/02/severe-vulnerabilities-patched-in-nextgen-gallery-affect-over-800000-wordpress-sites/
Infected Technology	WordPress NextGen Gallery Plugin version < 3.5.0
CVE-ID	CVE-2020-35942
Recommendation	Consider upgrading to a patched version of WordPress Gallery Plugin i.e., 3.5.0

8. A Windows Defender Vulnerability Lurked Undetected for 12 Years

Description	
A critical 12-year-old bug in Microsoft's ubiquitous Windows Defender antivirus was seemingly overlooked by attackers and defenders alike until recently. Now that Microsoft has finally patched it. The flaw showed up in a driver that Windows Defender—renamed Microsoft Defender last year—uses to delete the invasive files and infrastructure that malware can create. This bug allows privilege escalation. The vulnerability can only be exploited when an attacker already has access—remote or physical—to a target device. This means it isn't a one-stop-shop for hackers and would need to be deployed alongside other exploits in most attack scenarios.	
Source	https://labs.sentinelone.com/cve-2021-24092-12-years-in-hiding-a-privilege-escalation-vulnerability-in-windows-defender/
Infected Technology	Windows Defender
CVE- ID	CVE-2021-24092
Recommendation	Run an updated version of Windows Defender

9. Slack on Android users might have to reset their password

Description	
If you just got an email from Slack explaining that you need to reset your password with a big, phishy-looking link, it's legit. The company's Android app was accidentally logging credentials in plain text, and affected customers are being notified via email to reset their passwords. Slack says that only a small subset of users was affected. The company notes that there is no evidence to suggest that this data was accessed by third-parties. The bug has now been fixed and the affected app version has been blocked. If you were affected by this bug, you should receive an email from the company soon. Even otherwise, it might be wise to reset your password if you sign in to Slack manually.	
Source	https://www.androidpolice.com/2021/02/05/that-slack-email-you-just-got-asking-to-reset-your-password-is-legit-not-a-scam/
Infected Technology	Slack (Android App)
Recommendation	Consider resetting the password

10. LodaRAT Windows malware targets Android devices

Description	
Loda, an AutoIt malware that was implemented to perform phishing lures for executing a wide range of commands to capture sensitive information, record audio, and video is now found impacting Android services. Cisco Talos researchers have identified the new iteration of LodaRAT with improved sound recording capabilities. The latest versions are referred to as Loda4Andriod and Loda4Windows. These versions contain all the data-gathering features and stalk a constitute application. The Android variant of LODA behaves differently as it avoids techniques used by the banking trojans. The malware can take photos and screenshots, send SMS and perform calls, read SMA and call logs and intercept SMS messages or phone calls. The malware sends the information to a command-and-control(C2) server and has targeted banks and software companies based in Morocco.	
Source	https://blog.talosintelligence.com/2021/02/kasablanka-lodarat.html
Infected Technology	Android
Recommendation	Do not visit untrusted weblinks Do not download files from unknown sources

11. Siemens Patches 21 More File Parsing Vulnerabilities in PLM Products

Description

Siemens has released version V13.1.0.1 for JT2Go and Teamcenter Visualization to fix multiple vulnerabilities that could be triggered when the products read files in different file formats (PAR, BMP, TIFF, CGM, TGA, PCT, HPG, PLT, RAS, ASM, DGN, DXF, DWG). If a user is tricked into the opening of a malicious file with the affected products, this could lead to an application crash, or potentially arbitrary code execution or data extraction on the target host system. All of these vulnerabilities are related to how certain types of files are parsed by these products. An attacker can exploit them for arbitrary code execution, data extraction, and DoS attacks if they can trick the targeted user into opening a malicious file. Many of the issues affect the Siemens products due to their use of the Open Design Alliance (ODA) Drawings SDK. The ODA has published its advisory for the flaws.

Source	https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications
Infected Technology	JT2Go, Teamcenter Visualization
CVE-ID	CVE-2020-26998, CVE-2020-26999, CVE-2020-27000, CVE-2020-27001, CVE-2020-27002, CVE-2020-27003, CVE-2020-27004, CVE-2020-27005, CVE-2020-27006, CVE-2020-27007, CVE-2020-27008, CVE-2020-28394, CVE-2020-26989, CVE-2020-26990, CVE-2020-26991, CVE-2021-25173, CVE-2021-25174, CVE-2021-25175, CVE-2021-25176, CVE-2021-25177, CVE-2021-25178
Recommendation	Consider updating the products to its latest version.

12. Microsoft patches SharePoint, Excel RCE bugs in Office February security updates

Description
Microsoft has addressed severe remote code execution (RCE) vulnerabilities affecting the office products in January 2021 Office update. Microsoft released 26 security updates and 5 cumulative updates for 7 different products. The security updates have fixed 11 vulnerabilities that allowed attackers to execute arbitrary code remotely and escalate privileges on the systems running the vulnerable software. The windows systems running Click to Run and Microsoft Installer (.msi)-based edition of Microsoft Office products were vulnerable to RCE, information disclosure, and spoofing attacks due to the exposure of bugs. The six RCE bugs patched were rated as Important security issue by Microsoft that enabled attackers to execute arbitrary code for the currently logged-in user. The successful exploitation of these vulnerability lets an attacker install malicious programs, change and delete data and make a new admin account on the exploited Windows devices.

Source	https://support.microsoft.com/en-us/topic/february-2021-updates-for-microsoft-office-a21d8d13-c995-4e46-8573-3edd4f7e8499
Infected Technology	Microsoft Office Excel and SharePoint
CVE-ID	CVE-2021-24067, CVE-2021-24068, CVE-2021-24069 CVE-2021-24070, CVE-2021-24071, CVE-2021-1726 CVE-2021-24066, CVE-2021-24072
Recommendation	Consider installing Microsoft Office security updates through Microsoft's Download Center or Microsoft Update Platform

For any queries/recommendations:

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