January 18, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Microsoft issues patch for Defender Zero-Day and 82 Other Windows Flaws
- Windows 10 bug corrupts your hard drive
- Microsoft fixes Secure boot bug allowing Windows rootkit installation
- Windows Finger Command Abused by Phishing to Download Malware
- Millions of Social Profiles Leaked by Chinese Data-Scrapers
- BIG-IP product from F5 Networks can be exploited to launch remote denial-of-service (DoS) attacks.
- Critical Bug Found in WordPress Plugin called 'Orbit Fox' Allows Site Takeover
- Government site using apache velocity Tools Vulnerable to XSS

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 patch for Defender Zero-Day and 82 Other Windows Flaws

Description	
Microsoft released security updates that addressed 83 flaws affecting 11 products and services that included an actively exploited zero-day vulnerability on the first patch Tuesday of 2021. Among the 83 flaws, 10 were identified as Critical and 73 were identified as Important in severity. The most severe issue is a remote code execution (RCE) flaw present in Microsoft Defender that allowed attackers to penetrate a target system by executing arbitrary code. The patch solves a privilege escalation flaw in GDI Print / Printer Spooler API, memory corruption flaws in Microsoft Edge browser, Core Security Feature bypass flaw in Windows Remote Desktop Protocol and five RCE flaws in Remote Procedure Call Runtime.	
Source	https://msrc.microsoft.com/update-guide/releaseNote/2021-Jan
Infected Technology	Microsoft Windows Microsoft Edge (EdgeHTML-based) Microsoft Office and Microsoft Office Services and Web Apps Microsoft Windows Codecs Library Visual Studio SQL Server Microsoft Malware Protection Engine .NET Core .NET Repository ASP .NET Azure
CVE_ID	CVE-2020-26870, CVE-2021-1636, CVE-2021-1637, CVE-2021-1643, CVE-2021-1644, CVE-2021-1645, CVE-2021-1647, CVE-2021-1648, CVE-2021-1656, CVE-2021-1663, CVE-2021-1669, CVE-2021-1670, CVE-2021-1672, CVE-2021-1676, CVE-2021-1677, CVE-2021-1694, CVE-2021-1696, CVE-2021-1699, CVE-2021-1707, CVE-2021-1708, CVE-2021-1711, CVE-2021-1713, CVE-2021-1714, CVE-2021-1715, CVE-2021-1716, CVE-2021-1725
Recommendation	Install the latest security Windows update.

2. Windows 10 bug corrupts your hard drive

Description	
An unpatched zero-day vulnerability in Microsoft Windows 10 allows attacker to corrupt a hard drive in NTFS-format. The one-line command was hidden inside a ZIP archive to trigger hard drive errors that corrupted the filesystem index instantly. An attacker would sneak the malicious shortcut file with legitimate files inside a ZIP archive to entice the users to download the file. The file would not be triggered as an exploit as the contents of the ZIP file would be compressed and possibly encrypted. The BleepingComputer has reached out the Microsoft about the bug however, the InfoSEC community stress that such vulnerabilities remain unpatched after being known for years and been reported to Microsoft.	
Source	https://www.bleepingcomputer.com/news/security/windows-10-bug-corrupts-your-hard-drive-on-seeing-this-files-icon/
Infected Technology	Microsoft Windows 10

3. Microsoft fixes Secure boot bug allowing Windows rootkit installation

Description	
Microsoft fixes a security feature bypass vulnerability in Secure Boot. The vulnerability allowed attackers to compromise the booting process of the operating system even if Secure boot is enabled. The rootkit install is used by attackers to inject malicious code in computer's UEFI firmware, replace the boot loader of operating system, replace parts of Windows kernel or camouflage maliciously crafted Windows driver. The successful exploitation of the Secure Boot bug allows attackers to bypass secure boot and load untrusted software such as rootkits.	
Source	https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process#the-threat-rootkits
Infected Technology	Windows 10 release (from v1607 to v 1909) Windows 8.1 Windows Server 2012 R2 Windows Server 2012
CVE-ID	CVE-2020-0659
Recommendation	Use Secure Boot Forbidden Signature Database (DBX). Install the KB4535680 standalone update released by Microsoft (part of January 2021 Patch Tuesday). Manually install the January 2021 Security Updates.

4. Windows Finger Command Abused by Phishing to Download Malware

Description	
Attackers are using the normally harmless Windows Finger command to download and install a malicious backdoor on victims' devices. The 'Finger' command is a utility that originated in Linux/Unix operating systems that allows a local user to retrieve a list of users on a remote machine or information about a particular remote user. In addition to Linux, Windows includes a finger.exe command that performs the same functionality. As Finger is rarely used today, it is suggested that administrators block the Finger command on their network, whether through AppLocker or other methods.	
Source	http://hyp3rlinx.altervista.org/advisories/Windows_TCPIP_Finger_Command_C2_Channel_and_Bypassing_Security_Software.txt
Infected Technology	Windows OS
Recommendation	Consider blocking the Finger command in the network.

5. Apple Kills MacOS Feature Allowing Apps to Bypass Firewalls

Description	
Apple has removed a contentious macOS feature that allowed some Apple apps to bypass content filters, VPNs and third-party firewalls. The feature, first uncovered in November in a beta release of the macOS Big Sur feature, was called "ContentFilterExclusionList" and included a list of at least 50 Apple apps – including Maps, Music, FaceTime, the App Store and its software update service. It has recently been removed from the macOS Big Sur version 11.2. After discovering the undocumented exclusion list back in November, security researchers criticized Apple, saying it was a liability that can be exploited by threat actors to bypass firewalls, give them access to people's systems and expose their sensitive data.	
Source	https://www.patreon.com/posts/46179028
Infected Technology	MacOS Big Sur (Beta Release)
Recommendation	Upgrade MacOS Big Sur from its Beta version to version 11.2

6. High-Severity Cisco Flaw Found in CMX Software for Retailers

Description	
Cisco fixed high-severity flaws tied to 67 CVEs overall, including ones found in its AnyConnect Secure Mobility Client and in its RV110W, RV130, RV130W, and RV215W small business routers. A high-severity flaw in Cisco's smart Wi-Fi solution for retailers could allow a remote attacker to alter the password of any account user on affected systems. The vulnerability is part of a number of patches issued by Cisco addressing 67 high-severity CVEs on Wednesday. The most serious flaw afflicts Cisco Connected Mobile Experiences (CMX), a software solution that is utilized by retailers to provide business insights or on-site customer experience analytics.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmxpe-75Asy9k
Infected Technology	Cisco CMX Software
CVE-ID	CVE-2021-1144, CVE-202101237, CVE-2021-1146, CVE-2021-1147, CVE-2021-1148, CVE-2021-1149, CVE-2021-1150
Recommendation	Avoid using Cisco RV110W, RV130, RV130W, and RV215W routers as these routers have entered end-of-life-process.

7. Critical Bug Found in WordPress Plugin called 'Orbit Fox' Allows Site Takeover

Description	
According to researchers at Word fence, two vulnerabilities were discovered in a WordPress plugin called Orbit Fox which could allow the attackers to inject malicious code into vulnerable websites and/or take control of a website. Out of the two vulnerabilities the first flaw is an authenticated privilege-escalation flaw that carries a CVSS bug-severity score of 9.9, where an authenticated attacker with contributor level access or above can elevate themselves to administrator status and potentially take over a WordPress site and the second bug with CVSS score of 6.4 is an authenticated stored cross-site scripting (XSS) issue that allows attackers with contributor or author level access to inject JavaScript into posts.	
Source	https://www.wordfence.com/blog/2021/01/multiple-vulnerabilities-patched-in-orbit-fox-by-themeisle-plugin/
Infected Technology	WordPress, Orbit Fox Plugin
Recommendation	Update to the latest version 2.10.3

8. Government site using apache velocity Tools Vulnerable to XSS

Description	
A security researcher Jackson Henry from sakura samurai ethical hacking group discovered an undisclosed Cross-Site Scripting (XSS) vulnerability in Apache Velocity Tools which can be exploited by unauthenticated attackers to target government sites, including NASA and NOAA. Apache Velocity is a Java-based template engine used by developers for designing *views* in a Model-View-Controller (MVC) architecture. Although a formal vulnerability disclosure has not taken place, Bleeping Computer has been informed that this flaw is being internally tracked as **CVE-2020-13959.** The reflected XSS flaw exists in how the Velocity View Servlet view class renders error pages. When an invalid URL is accessed, the "template not found" error page reflects the resource path portion of the URL *as it is* without escaping it for potential XSS scripts.	
Source	https://www.bleepingcomputer.com/news/security/undisclosed-apache-velocity-xss-vulnerability-impacts-gov-sites/?&web_view=true
Infected Technology	Apache Velocity Tools, Apache
CVE-ID	CVE-2020-13959
Recommendation	Update to the latest version

9. BIG-IP product from F5 Networks can be exploited to launch remote denial-of-service (DoS) attacks.

Description	
A cyber security researcher Nikita Abramov, from cybersecurity solutions provider Positive Technologies discovered a vulnerability in BIG-IP product from F5 Networks which can be exploited to launch remote denial-of-service (DoS) attacks. This flaw has a impact on certain versions of BIG-IP Access Policy Manager (APM), a secure access solution that simplifies and centralizes access to applications, APIs and data. According to F5 Networks, the vulnerability is related to a component named Traffic Management Microkernel (TMM), which processes all load-balanced traffic on BIG-IP systems.	
Source	https://www.securityweek.com/vulnerability-exposes-f5-big-ip-systems-remote-dos-attacks?&web_view=true
Infected Technology	Big-IP, F5 Networks
CVE-ID	CVE-2020-27716
Recommendation	Update to the latest patched version

10. Millions of Social Profiles Leaked by Chinese Data-Scrapers

Description	
More than 400GB of public and private profile data for 214 million social-media users from around the world has been exposed to the internet – including details for celebrities and social-media influencers in the U.S. and elsewhere. The leak stems from a misconfigured Elasticsearch database owned by Chinese social-media management company SocialArks, which contained personally identifiable information (PII) from users of Facebook, Instagram, LinkedIn and other platforms, according to researchers at Safety Detectives. The server was found to be publicly exposed without password protection or encryption during routine IP-address checks on potentially unsecured databases, researchers said. It contained more than 318 million records in total.	
Source	https://www.safetydetectives.com/blog/socialarks-leak-report/
Infected Technology	Elasticsearch Server, Facebook, LinkedIn, Instagram
Recommendation	Only give out what you feel confident cannot be used against you (avoid government ID numbers, personal preferences that may cause you trouble if made public, etc.) Check that the website you are on is secure (look for https and/or a closed lock) Do not click links in emails unless you are sure that the sender is legitimately who they represent themselves to be.

For any queries/recommendations:

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