June 21
2021

INFOSEC WEEKLY

#MADE4SECURITY

- Google Introduces Patch to Fix Another 0-Day Exploit
- Apple Release Patches for two Zero-Day Flaws3.
- Thousands of publicly accessible VMware vCenter Servers vulnerable to critical flaws
- Microsoft Teams: Very Bad Tabs Could Have Led to BEC (Business Email Compromise)
- Remote Code Execution Vulnerability found in Paint 3D
- A researcher discovered multiple vulnerabilities in smart switches of Cisco's Small Business 220 series

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. Google Introduces Patch to Fix Another 0-Day Exploit

Description	
Google has released another patch update to update Chrome browser for Windows, Mac, and Linux. This patch rectifies four vulnerabilities that include a zero-day flaw. The zero-day vulnerability is CVE tracked and has high severity flaw relating to a Web Graphics Library (WebGL) vulnerability. This library is used to render the graphics within the browser. The exploitation of the vulnerability could allow an attacker to corrupt the valid data, crash and allow to execute code and commands in an unauthorized setting. This issue was reported to Google by an anonymous individual that addressed the company that the exploit for this vulnerability exists within the internet.	
Source	https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_17.html
Infected Technology	Google Chrome
CVE ID	CVE-2021-30554
Recommendation	Install the latest security patch as soon as possible.

2. Apple Release Patches for two Zero-Day Flaws

Description	
Apple has released security patches that consider two zero-day vulnerabilities affecting iOS 12.5.3. The zero-day vulnerabilities include memory corruption and use-after-free issues. The memory corruption issue can be exploited to execute arbitrary code. The attacker would be able to execute malicious payload via specially crafted web content. The use-after-free issue exploitation could also lead to arbitrary code execution while processing web content malicious payloads. The vulnerabilities were reported by anonymous individuals stating that 'vulnerabilities might have been exploited'. Further detail of the exploitation has not been disclosed by Apple.	
Source	https://support.apple.com/en-us/HT212548
Infected Technology	• iPhone 5s, iPhone 6, iPhone 6 Plus • iPad Air, iPad mini 2, iPad mini 3 • iPod touch (6th generation)
CVE-ID	CVE-2021-30761, CVE-2021-30762
Recommendation	Update the Apple devices to the latest version available

3. **Thousands of publicly accessible VMware vCenter Servers vulnerable to critical flaws**	
Description	
After three weeks of releasing patches for two serious vulnerabilities that stem from the use of VMware vCenter plug-ins in VMware vCenter, thousands of servers that are reachable from the internet remain vulnerable to attacks. Researchers from security firm Trustwave recently identified 5,271 instances of VMware vCenter Server accessible from the internet among which vast majority of them (5,076) operate over port 443. A hacker with access to the server over port 443 (HTTPS) can exploit this issue without authentication to execute commands with unrestricted privileges on the operating system that hosts vCenter Server.	
Source	https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/thousands-of-vulnerable-vmware-vcenter-servers-still-publicly-exposed-cve-2021-21985-cve-2021-21986/
Infected Technology	• VMware vCenter Server versions 6.5, 6.7 and 7.0 • VMware Cloud Foundation 3.x and 4.x
CVE ID	CVE-2021-21985, CVE-2021-21986
Recommendation	• Consider installing the security patches provided by VMware. • Consider updating the infected products to their latest version.

4. Microsoft Teams: Very Bad Tabs Could Have Led to BEC (Business Email Compromise)	
Description	
On Monday, Tenable's Evan Grant explained in a post that he found the bug in Microsoft Power Apps: a platform for low-code/no-code rapid app development. As put by Evan, attackers could have stepped through a yawning security hole in the Microsoft Teams chat service that would have let them masquerade as a targeted company's employee, by reading and sending email on their behalf. Exploitation would require a lot of moving parts. But the bug is a simple one, having to do with insufficient input validation. The vulnerability could be leveraged to establish persistent read/write access to the victim's Microsoft bubble, including email, Teams chats, OneDrive, SharePoint, and a variety of other services. Such attacks could be carried out via a malicious Microsoft Teams tab and Power Automate flows. Microsoft has now fixed the bug but still is exploitable as put by Evan.	
Source	https://www.tenable.com/security/research/tra-2021-23
Infected Technology	Microsoft Teams
Recommendation	Consider updating to the latest version of Microsoft Teams.

5. Remote Code Execution Vulnerability found in Paint 3D	
Description	
The vulnerability in paint 3D allowed remote attackers to execute arbitrary code on affected installations. If the victim visited a rogue page or opened a malicious file, which required user involvement, then the attackers could exploit this issue. The problem in question is in the parsing of STL files. The problem arises from a lack of sufficient validation of user-supplied data, which might lead to a read past the end of a data structure that has been allocated. An attacker can use this flaw to execute code with low integrity in the context of the current process.	
Source	https://www.theregister.com/2021/06/16/3d_paint_vuln/?&web_view=true
Infected Technology	Microsoft's Paint 3D
CVE ID	CVE-2021-31946
Recommendation	Update the application to the latest version

6. A researcher discovered multiple vulnerabilities in smart switches of Cisco's Small Business 220 series	
Description	
Security researcher Jasper Lievisse Adriaanse has discovered multiple vulnerabilities in Cisco's Small Business 220 series smart switches. The vulnerabilities impact devices running firmware versions prior 1.2.0.6 and which have the web-based management interface enabled. The most severe one is a weak session management vulnerability that can allow a remote, unauthenticated attacker to hijack a user's session and access the web interface of the network device with privileges up to the level of the administrative user. Another high-severity issue is a remote command execution vulnerability that a remote attacker with admin permissions could exploit to execute arbitrary commands with root privileges on the underlying operating system. The remaining vulnerabilities are a Cross-Site Scripting (XSS) vulnerability and HTML injection vulnerability, both issues have been rated as medium severity.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E
Infected Technology	Cisco 220 series switches version < 1.2.0.6
CVE ID	CVE-2021-1541, CVE-2021-1542, CVE-2021-1543, CVE-2021-1571, CVE-2021-1542
Recommendation	Consider staying up to date with the software updates released by Cisco.

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/