July 12, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Microsoft Office Users Warned on New Malware-Protection Bypass
- Cisco BPA, WSA Bugs Allow Remote Cyberattacks
- Philips Vue vulnerable to Remote Code Execution
- Vulnerabilities in Sage X3 ERP allows execution of system command
- Android July Security Update patches over 40 vulnerabilities
- Remote Code Execution Vulnerability on Powershell

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 Office Users Warned on New Malware-Protection Bypass

Description	
Microsoft Excel legacy users are being targeted in a malware campaign that use a unique malware-obfuscation method to deactivate Office protections and deliver the Zloader trojan. The malicious attack combines features in Microsoft Office Word and Excel to work together to download the Zloader payload without raising an alert message for end users. Zloader is a banking trojan that is designed to steal login passwords and other sensitive information from users of certain financial institutions. The initial attack vector is inbox-based phishing mails with non-malicious Word document attachments. As a result, it is unlikely to trigger an email gateway or client-side antivirus software to prevent the attack.	
Source	https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zloader-with-a-new-infection-technique/
Infected Technology	Microsoft office Package
Recommendation	Do not enable macros on files from untrusted sources.

2. Cisco BPA, WSA Bugs Allow Remote Cyberattacks

Description	
A series of high-severity privilege-escalation vulnerabilities have been discovered in Cisco's Web Security Appliance (WSA), which works as a shield and automatically bans high-risk sites, as well as its Business Process Automation application. These flaws in the programs might provide a means for authenticated remote attackers to access sensitive data or hijack the system through Cisco BPA and WSA.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bpa-priv-esc-dgubwbH4 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-scr-web-priv-esc-k3HCGJZ
Infected Technology	• Cisco BPA earlier than 3.1 • Cisco WSA 11.8 and earlier, 12.0 and 12.5
CVE-ID	CVE-2021-1574, CVE-2021-1576, CVE-2021-1359
Recommendation	Apply the latest patch available.

3. Philips Vue vulnerable to Remote Code Execution

Description	
US's Cybersecurity and Infrastructure Security Agency (CISA) has released an advisory containing 15 vulnerabilities in Philips Vue healthcare product. The advisory contains four critical and four high severity vulnerabilities due to improper input validation, memory bugs, improper authentication, insecure/improper initialization of resources, use of expired cryptographic keys, use of weak cryptographic algorithms, improper use of protection mechanisms, data integrity issues, cross-site scripting (XSS), improperly protected credentials, and the cleartext transmission of sensitive data which can allow attacker to gain system access, execute arbitrary code and eavesdrops on the communication with ability to modify the data.	
Source	https://us-cert.cisa.gov/ics/advisories/icsma-21-187-01
Infected Technology	• Vue PACS: Versions 12.2.x.x and prior • Vue MyVue: Versions 12.2.x.x and prior • Vue Speech: Versions 12.2.x.x and prior • Vue Motion: Versions 12.2.1.5 and prior
CVE_ID	CVE-2020-1938, CVE-2018-12326, CVE-2018-11218, CVE-2020-4670, CVE-2018-8014, CVE-2021-33020, CVE-2018-10115, CVE-2021-27501, CVE-2021-33018, CVE-2021-27497, CVE-2012-1708, CVE-2015-9251, CVE-2021-27493, CVE-2019-9636, CVE-2021-33024, CVE-2021-33022
Recommendation	• Apply the update released by OEM which addresses some of the flaws • Apply update after the full patch has been released

4. Vulnerabilities in Sage X3 ERP allows execution of system command

Description	
Researchers from Rapid7 has identified four vulnerabilities in Sage X3 product, one of which has a CVSS score of 10. The vulnerabilities when left unpatched can allow threat actor to execute system command and take over the system, while other vulnerabilities include XSS, missing authentication and exposure of sensitive data. The identified vulnerabilities have been fixes in recent release and users are urged to update to the latest version as the proof of concept has been released.	
Source	https://www.rapid7.com/blog/post/2021/07/07/cve-2020-7387-7390-multiple-sage-x3-vulnerabilities/
Infected Technology	Sage X3
CVE_ID	CVE-2020-7388, CVE-2020-7387, CVE-2020-7389, CVE-2020-7390
Recommendation	Apply the update released by OEM

5. Android July Security Update patches over 40 vulnerabilities

Description	
Google has announced release of July 2021 security update that patches over 40 security vulnerabilities. Seven of the vulnerabilities mentioned are rated critical while most of the remaining are high severity vulnerabilities. The exploitation of the existing vulnerabilities could allow attacker with specially crafted file to execute arbitrary code and elevate user privilege.	
Source	https://source.android.com/security/bulletin/2021-07-01
Infected Technology	Android 8, 9, 10
Recommendation	Apply the security update once released by your Smartphone OEM

6. Remote Code Execution Vulnerability on Powershell

Description	
PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework and currently a new issue has been tracked as CVE-2021-26701 that affects Powershell version 7.0 and 7.1. The impact of the mentioned CVE is a remote code execution on vulnerable versions and Microsoft has requested Azure users to update the tool as soon as possible.	
Source	https://azure.microsoft.com/en-us/updates/update-powershell-versions-70-and-71-to-protect-against-a-vulnerability/
Infected Technology	Microsoft Powershell 7.0 & 7.1
CVE-ID	CVE-2021-26701
Recommendation	Update powershell version to 7.0.6 or 7.1.3

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/