February 01, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Sudo Bug Gives Root Access to Mass Numbers of Linux Systems
- IBM QRadar SIEM is vulnerable to Server-Side Request Forgery (SSRF)
- Apple Warns of 3 iOS Zero-Day Security Vulnerabilities Exploited in the Wild
- Cisco DNA Center Bug Opens Enterprises to Remote Attack
- Google fixes severe Golang Windows RCE vulnerability
- DDoS Attackers Exploit Vulnerable Microsoft RDP Servers
- New Wormable Android Malware Spreading through WhatsApp
- CrowdStrike Discloses Details of Recently Patched Windows NTLM Vulnerability

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. Sudo Bug Gives Root Access to Mass Numbers of Linux Systems

Description	
The Sudo privilege escalation vulnerability was discovered by security researchers from Qualys, who disclosed it on January 13th and made sure that patches are available before going public with their findings. A now-fixed Sudo vulnerability allowed any local user to gain root privileges on Unix-like operating systems without requiring authentication. According to Qualys researchers, the issue is a heap-based buffer overflow exploitable by any local user (normal users and system users, listed in the sudoers file or not), with attackers not being required to know the user's password to successfully exploit the flaw. The buffer overflow allowing any local user to obtain root privileges is triggered by Sudo incorrectly unescaping backslashes in the arguments.	
Source	https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit
Infected Technology	Linux/Unix Based Operating Systems
CVE-ID	CVE-2021-3156
Recommendation	Consider upgrading Sudo to version 1.9.5p2

2. IBM QRadar SIEM is vulnerable to Server-Side Request Forgery (SSRF)

Description	
IBM QRadar is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. The RssFeedItem class of the QRadar web application is used to fetch and parse RSS feeds. No validation is performed on the user-supplied RSS feed URL. Due to the lack of URL Validation, authenticated attacker can execute Server-Side Request Forgery attacks. Using this issue, it is possible to call the Apache Axis AdminService webservice to execute arbitrary code with the privileges of the Tomcat user.	
Source	https://www.ibm.com/support/pages/node/6408864
Infected Technology	• IBM QRadar SIEM 7.4.2 GA • IBM QRadar SIEM 7.4.0 • IBM QRadar SIEM 7.3.0
CVE-ID	CVE-2020-4787
Recommendation	Consider applying the patches provided by IBM.

3. Apple Warns of 3 iOS Zero-Day Security Vulnerabilities Exploited in the Wild

Description

On Tuesday, Apple released updates for iOS, iPadOS, and tvOS with fixes for three security vulnerabilities that may have been actively exploited. The three zero-day flaws could have allowed an attacker to elevate privileges and achieve remote code execution. The privilege escalation bug in the kernel (CVE-2021-1782) was noted as a race condition that could cause a malicious application to elevate its privileges. Furthermore, the other two issues were discovered in the WebKit browser engine (CVE-2021-1870 and CVE-2021-1871) that could permit an attacker to achieve arbitrary code execution inside Safari. According to Apple, the race condition and the WebKit flaws have been addressed with improved locking and restrictions.

Source	https://support.apple.com/en-us/HT212146 https://support.apple.com/en-us/HT212149
Infected Technology	iOS 14.4, iPadOS 14.4, and tvOS 14.4
CVE-ID	CVE-2021-1782, CVE-2021-1870, CVE-2021-1871
Recommendation	Consider installing security updates provided by Apple.

4. Cisco DNA Center Bug Opens Enterprises to Remote Attack

Description

A cross-site request forgery (CSRF) vulnerability in the Cisco Digital Network Architecture (DNA) Center could open enterprise users to remote attack and takeover. The flaw exists in the web-based management interface of the Cisco DNA Center, which is a centralized network-management and orchestration platform for Cisco DNA. An attacker could exploit the vulnerability by socially engineering a web-based management user into following a specially crafted link, say via a phishing email or chat. If the user clicks on the link, the attacker can then perform arbitrary actions on the device with the privileges of the authenticated user.

Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-csrf-dC83cMcV
Infected Technology	Cisco DNA Center version < 2.1.1.0
CVE_ID	CVE-2021-1257
Recommendation	Consider applying the patch provided by Cisco.

5. Google fixes severe Golang Windows RCE vulnerability

Description	
Recently, a command injection vulnerability was discovered in the Golang project. The RCE vulnerability mainly impacts Windows users of Go running the “go get” command, due to the default behavior of Windows PATH lookups. It stems from how the compile process works when a user runs the "go get" command to fetch a repository. The critical command injection vulnerability in Git LFS, CVE-2020-27955, inspired the researcher to hunt for a similar flaw in Golang itself. It requires some interaction by the victim. For a remote attacker to exploit this vulnerability, a user needs to run the “go get” command against a malicious repository. The Golang team at Google has fixed the vulnerability and users are advised to upgrade their instances.	
Source	https://groups.google.com/g/golang-announce/c/mperVMGa98w
Infected Technology	• Go version < 1.14.14 • Go version < 1.15.7
CVE -ID	CVE-2021-3115
Recommendation	Upgrade Go to its latest version available.

6. DDoS Attackers Exploit Vulnerable Microsoft RDP Servers

Description	
Netscout researchers have identified about 33,000 vulnerable Microsoft RDP servers that could be abused by threat actors to boost their DDoS attacks. The researchers found that when the Microsoft RDP service is configured to UDP port 3389, attacks could amplify network packets from vulnerable ports and redirect that traffic to targeted IP addresses, increasing the size of a DDoS attack at little cost. In some cases, the NetScout researchers found an amplification ratio of 85.9:1, which means that for every 10 gigabytes per second of requests directed at an RDP server, the threat actors could redirect 860 gigabytes per second of network traffic at the targeted IP address as part of the DDOS attack.	
Source	https://www.netscout.com/blog/asert/microsoft-remote-desktop-protocol-rdp-reflectionamplification
Infected Technology	Microsoft Remote Desktop Protocol (RDP) servers
Recommendation	Ensure that RDP servers are protected behind a VPN service.

7. New Wormable Android Malware Spreading through WhatsApp

Description	
According to the malware researcher Lukas Stefanko at cybersecurity firm ESET, A new wormable malware has been found that propagates itself through WhatsApp messages to other contacts. This malware spreads via the victim's WhatsApp by automatically replying to any received WhatsApp message notification with a link to [a] malicious Huawei Mobile app. The link to the fake Huawei Mobile app, upon clicking, redirects users to a lookalike Google Play Store website. Once installed, the wormable app prompts victims to grant it notification access, which is then abused to carry out the wormable attack. Specifically, it leverages WhatApp's quick reply feature which is used to respond to incoming messages directly from the notifications to send out a reply to a received message automatically.	
Source	https://thehackernews.com/2021/01/beware-new-wormable-android-malware.html
Infected Technology	All smartphones using WhatsApp
Recommendation	Consider downloading apps only from the google play store.

8. CrowdStrike Discloses Details of Recently Patched Windows NTLM Vulnerability

Description	
Microsoft on its January 2021 Patch Tuesday addressed a vulnerability that allows an attacker to relay NTLM authentication sessions and then execute code remotely, using a printer spooler MSRPC interface. The vulnerability has been described by Microsoft as an NT LAN Manager (NTLM) security bypass and is rated Important for all affected Windows versions. In the blog post detailing the issues, CrowdStrike explains that NTLM relay attack methods are not uncommon and that relaying NTLM authentications to another protocol like SMB, LDAP/S, and MSRPC is possible when required protection are not present.	
Source	https://www.crowdstrike.com/blog/cve-2021-1678-printer-spooler-relay-security-advisory/
Infected Technology	Windows Server 2012 R2, Server 2008, Server 2016, Server 2019, RT 8.1, 8.1, 7, and 10
CVE_ID	CVE-2021-1678

9. QNAP Network Devices Targeted by New Dovecat Malware

Description	
QNAP urges customers to secure their network-attached storage (NAS) devices against an ongoing malware campaign that infects and exploits them to mine bitcoin without their knowledge. QNAP says, "According to analysis, QNAP NAS can become infected when they are connected to the Internet with weak user passwords". After the company started receiving reports from its users, last year, concerning two unknown processes (dovecat and dedpma), the security advisory was released. The malware can infect Linux systems. However, it has been specially created to target the internal structure of the QNAP NAS device. It propagates via targeting weak passwords.	
Source	https://cyware.com/news/qnap-network-devices-targeted-by-new-dovecat-malware-950680eb
Infected Technology	QNAP Network-Attached Storage (NAS) Devices
Recommendation	• Consider updating QTS to the latest version. • Consider using a strong admin password.

10. WordPress sites affected by 'Popup Builder' plugin vulnerabilities

Description	
Pop Builder, a plugin allowing WordPress site owners to create, customize and manage promotion modal popups, with over 200,000 installations is found to be vulnerable. Researchers at WebARX have addressed this issue which is caused by the lack of authorization on most AJAX methods. The missing authorization creates security flaws that can be leveraged to send out a newsletter, import or delete subscribers, local file inclusion, and other actions. The vulnerable methods can be exploited by an authenticated user to send newsletters with custom body, email sender, and other attributes hence, allowing a malicious user to send emails to the subscribers. This vulnerability could provide serious damage to the reputation and security status of the website	
Source	https://www.webarxsecurity.com/multiple-vulnerabilities-wordpress-plugin-popup-builder/
Infected Technology	Popup Builder 3.71 and below.
Recommendation	Update the plugin to the latest version 3.73.

11. Industrial Firms Informed About Serious Vulnerabilities in Matrikon OPC Product.

Description	
As part of OPC UA security analysis, researchers at industrial cybersecurity firm Claroty discovered that Matrikon's OPC UA Tunneling products, which was designed for integrating OPC UA clients and servers with OPC Classic architecture, is affected by four critical and high-severity vulnerabilities that can be exploited for remote code execution, DoS attacks, and for obtaining potentially valuable information. Most of them can be exploited to crash a server, and some, under certain conditions, can result in remote code execution. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) last week published an ICS advisory to inform industrial organizations about these vulnerabilities.	
Source	https://us-cert.cisa.gov/ics/advisories/icsa-21-021-03
Infected Technology	Matrikon OPC Product
CVE-ID	CVE-2020-27297, CVE-2020-27299, CVE-2020-27274, CVE-2020-27295
Recommendation	Consider upgrading Matrikon OPC UA Tunneller to Version 6.3.0.8233.

12. YouPHPTube and AVideo vulnerabilities could lead to RCE

Description	
Security researchers from Synacktiv have found multiple vulnerabilities in the source codes of open-source video platforms YouPHPTube and AVideo. The vulnerabilities had arisen in the project due to improper input sanitization. The vulnerabilities could be leveraged to execute remote code execution (RCE) in the user's device. The verified vulnerabilities include unauthenticated SQL injection, multiple cross-site scripting (XSS) flaws, and file write vulnerability. The SQL injection vulnerability could lead the attackers to export sensitive data (password hashes) and allow an unauthenticated user to have administrative privileges. The reflected XSS could lead to exposure of the administrator's session cookies and perform tasks as an administrator. File write flaw allows the administrator to execute malicious code on the server.	
Source	https://www.synacktiv.com/sites/default/files/2021-01/YouPHPTube_Multiple_Vulnerabilities.pdf
Infected Technology	• YouPHPTube versions 7.8 and below • AVideo versions 10.0 and below

13. Blind TCP/IP hacking for Windows 7

Description
Windows 7 has been identified as susceptible to blind TCP/IP hijacking attackers that were reported to Microsoft 8 years ago. The attack is executed via a vulnerability that was identified in a blog post written in 2008. As Windows 7 was released in 2009, it will no longer receive security updates as it has reached the end of life in 2019. The bug present in Windows 7 allows the attacker to use the machine as a zombie host. The attacker would be invisible to the target and can fully hijack an established TCP connection present on the system. The protocols that do not encrypt traffic: FTP, HTTP, DNS, IMAP., SMTP, and more permits an attacker to send commands on behalf of the original client. The TELNET protocols used in most IoT devices could face catastrophic impact by the hijacking of the session.

Source	http://blog.pi3.com.pl/?p=850
Infected Technology	Windows 7

14. Multiple vulnerabilities in phpGACL class

Description
Cisco Talos recently discovered multiple vulnerabilities in the phpGACL class. One of these vulnerabilities also affects OpenEMR, a medical practice management software written in PHP. phpGACL is a PHP library that allows developers to implement permission systems via a Generic Access Control List. An adversary could exploit these vulnerabilities by sending the target machine a specially crafted, malicious HTTP request or URL. Some of the discovered vulnerabilities are phpGACL template multiple cross-site scripting vulnerabilities, phpGACL return_page redirection open redirect vulnerability, phpGACL database multiple SQL injection vulnerabilities, and OpenEMR GACL cross-site request forgery vulnerability.

Source	https://blog.talosintelligence.com/2021/01/vuln-spotlight-php-gacl-openemr.html?&web_view=true
Infected Technology	• PHP, phpGACL openEMR
CVE-ID	CVE-2020-13562, CVE-2020-13564, CVE-2020-13565, CVE-2020-13566, CVE-2020-13568, CVE-2020-13569
Recommendation	• Consider using the openEMR later version after 5.0.2, development version 6.0.0 and phpGACL version 3.3.7. • If you are using Snort then consider implementing Snort Rules: 56143 - 56149, 56152, 56153.

15. Remote Code Execution vulnerability discovered in Node.js apps

Description	
A security researcher "captain freak" found a vulnerability in a Node.js web application framework that could be exploited to achieve remote code execution (RCE). He also suggested that Express.js may be susceptible to local file read errors and when combined with an old version of the Handlebars engine, this flaw could also be exploited to remotely execute malicious code.	
Source	https://blog.shoebpatel.com/2021/01/23/The-Secret-Parameter-LFR-and-Potential-RCE-in-NodeJS-Apps/
Infected Technology	Node, Express.js
Recommendation	Consider using Handlebars versions 4.1.2, 4.0.14, and later.

16. Nvidia has patched several vulnerabilities affecting its Jetson Products

Description	
Nvidia has patched three vulnerabilities affecting its Jetson lineup, which is a series of embedded computing boards designed for machine-learning applications, in things like autonomous robots, drones, and more. If exploited, the most serious of these flaws could lead to a denial-of-service (DoS) condition for affected products. Out of the three vulnerabilities, Nvidia Linux Driver Package (L4T) flaw (CVE-2021-1070) ranks 7.1 out of 10 on the CVSS scale, making it high-severity in which an unprivileged user can modify system device tree files, leading to a denial of service. The other two are medium-severity flaws (CVE-2021-1069 and CVE-2021-1071), which were uncovered in the Nvidia Tegra's kernel driver where CVE-2021-1069 exists in NVHost leading to data loss and CVE-2021-1071 meanwhile exists in the INA3221 driver which may lead to unauthorized users gaining access to system power usage data. This can lead to information disclosure.	
Source	https://nvidia.custhelp.com/app/answers/detail/a_id/5147
Infected Technology	• NVIDIA, Jetson
CVE-ID	CVE-2021-1070, CVE-2021-1069, CVE-2021-1071
Recommendation	• Consider updating it to its latest version.

For any queries/recommendations:

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