January 11, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Git misconfiguration leaks Nissan source code online
- Fortinet updates WAF to protect against SQL injection, DoS attacks
- NVIDIA fixes security flaw affecting Windows and Linux devices
- New Golang Worm Drops XMRig Miner
- Cybercriminals are targeting GitHub Service to Host Malware
- Google Warns of Critical Android Remote Code Execution Bug
- RCE Bug Found and Disputed in Popular PHP Scripting Framework

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. Git misconfiguration leaks Nissan source code online

Description

Source codes of mobile apps and internal tools developed by North America based Nissan has been leaked online due to misconfiguration in one GIT server. Tillie Kottmann, a Switzerland-based software engineer stated that the leak was originated from a Bitbucket instance GIT server that used default username and password combination: **admin/admin**. The leaked repositories contained the source codes of multiple application related to mobile apps, diagnostic tools, core mobile library, marketing tools, sales/market research and various other backend and internal tools. The Bitbucket instance Git server was taken offline as the leaked data was circulated in the torrent sites, hacking forums and telegram channels.

Source	https://twitter.com/antiproprietary/status/1346238602536214528
Infected Technology	Git Server
Recommendation	Update the password of critical application according to the password policy standards provided by the company or NIST.

2. Fortinet updates WAF to protect against SQL injection, DoS attacks

Description

Fortinet has resolved various vulnerabilities in its network security appliances. FortiWeb Web Application Firewall (WAF) was vulnerable to SQL injection. The vulnerability in the UI of FortiWeb allowed unauthenticated remote attackers to execute SQL arbitrary queries or commands. The vulnerable network infrastructure led to the execution of unauthorized codes and command hence, a critical risk to an important component of network security

Source	https://www.fortiguard.com/psirt/%20FG-IR-20-124
Infected Technology	FortiWeb versions 6.3.7 and below. FortiWeb versions 6.2.3 and below.
CVE-ID	CVE-2020-29015
Recommendation	Upgrade to the following FortiWeb versions: • 6.3.8 or above • 6.2.4 or above

3. NVIDIA fixes security flaw affecting Windows and Linux devices

Description

NVIDIA has released security updates to address six security vulnerabilities present in Windows and Linux GPU display drivers and ten additional flaws affecting the NVIDIA Virtual GPU (vGPU) management software. If exploited, the vulnerabilities could lead to denial of service (DoS), privilege escalation, data tampering and information disclosure in the effected Linux or Windows machines. The security issues require local user access hence, the attackers are initially required to gain access to the vulnerable devices. The vulnerabilities exploitation could also lead to the possibility of running vulnerable drivers and software to hamper the workflow and gaining access to unobtainable information.

Source	https://nvidia.custhelp.com/app/answers/detail/a_id/5142/kw/Security%20Bulletin
Infected Technology	NVIDIA GPU drivers and Virtual GPU management software.
CVE-ID	CVE-2021-1052, CVE-2021-1053, CVE-2021-1056
Recommendation	Update the NVIDIA GPU and Virtual GPU manager software from the following link: https://www.nvidia.com/Download/index.aspx

4. New Golang Worm Drops XMRig Miner

Description

A researcher from Intezer discovered a new and self-spreading Golang-based malware [new crypto-mining malware] which exploits known vulnerabilities to exploit the victim's resources. The attack uses three files: a dropper script (bash or PowerShell), a Golang-based worm, and drop XMRig miner on the exploited service. The worm targets public-facing services such as Jenkins, MySQL, and Tomcat admin panel that have weak passwords and scans the network using TCP SYN to launch credential spraying brute force attack and spreads over the network.

Source	https://cyware.com/news/new-golang-worm-drops-xmrig-miner-8ae0bdf1
Infected Technology	Jenkins, MYSQL, Tomcat, Windows, linux
Recommendation	• Consider to use complex passwords. • Consider to use multi-factor authentication to protect against such cyber-threats. • Consider to limit login attempts.

5. Cybercriminals are targeting GitHub Service to Host Malware

Description

One of the famous Open-source software repositories is being actively abused by the attackers to host and distribute their malicious components and malware. A recent report, from Octoverse revealed that almost a fifth (around 17%) of all software bugs in GitHub were intentionally placed as backdoors by cybercriminals in which the majority of these backdoors came from the npm ecosystem that affected many projects depending on those packages.

Source	https://octoverse.github.com/#securing-software
Infected Technology	Github

6. Google Warns of Critical Android Remote Code Execution Bug

Description

Google has fixed two critical bugs affecting its Android handsets. The more serious flaws exist in the Android System component and allow remote attackers to execute arbitrary code. The two critical vulnerabilities are part of Google's January Android security bulletin, released Monday. The security update addressed 43 bugs overall for the Android operating systems. As part of this, Qualcomm, whose chips are used in Android devices, patched a mix of high- and critical-severity vulnerabilities tied to 15 bugs.

Source	https://threatpost.com/google-warns-of-critical-android-remote-code-execution-bug/162756/
Infected Technology	Android versions 8.0, 8.1, 9, 10, 11
CVE-ID	CVE-2021-0316, CVE-2021-0303, CVE-2021-0306, CVE-2021-0307, CVE-2021-0310, CVE-2021-0315, CVE-2021-0313, CVE-2021-0317, CVE-2021-0318, CVE-2021-0319, CVE-2021-0304
Recommendation	Apply the security patches provided by google.

7. RCE Bug Found and Disputed in Popular PHP Scripting Framework

Description	
Versions of the popular developer tool Zend Framework and its successor Laminas Project can be abused by an attacker to execute remote code on PHP-based websites, if they are running web-based applications that are vulnerable to attack. However, those that maintain Zend Framework emphasize that the conditions under which a web app can be abused first require the application author to write code that is "inherently insecure." For that reason, the current maintainers of Zend Framework are contesting whether the vulnerability classification is correct.	
Source	https://threatpost.com/rce-bug-php-scripting-framework/162773/
Infected Technology	Zend Framework, version = 3.0.0 Laminas Project, version < 2.14.2
Recommendation	Apply patches available for Zend Framework and Laminas Project.

8. Cybercriminals Ramp Up Exploits Against Serious Zyxel Flaw

Description	
Security experts are warning about hackers ramping up to exploit a high severity vulnerability that may still reside in over 100,000 Zyxel Communications products. Zyxel, a Taiwanese manufacturer of networking devices, on Dec 23 warned the flaw in its firmware and released patches to address the issue. Zyxel device are generally utilized by small business as firewalls and VPN gateways. The vulnerability stems from Zyxel devices containing an undocumented account (called zyfwp) that has an unchangeable password – which can be found in cleartext in the firmware.	
Source	https://threatpost.com/cybercriminals-exploits-zyxel-flaw/162789/
Infected Technology	Zyxel networking products
CVE-ID	CVE-2020-29583
Recommendation	Apply security patches provided by Zyxel.

9. NSA Urges SysAdmins to Replace Obsolete TLS Protocols.

Description

The National Security Agency (NSA) is urging SysAdmins to replace insecure and outdated Transport Layer Security (TLS) protocol instances. The agency this week released new guidance and tools to equip companies to update from obsolete older version of TLS (TLS 1.0 and TLS 1.1) to newer versions of protocol (TLS 1.2 or TLS 1.3). As of March 2020, more than 850,000 websites still used TLS 1.0 and 1.1 protocols. Meanwhile, according to the SANS ISC in December, TLS 1.3 is supported by about one in every five HTTPS server, showing steady adoption of the newer protocol version.

Source	https://threatpost.com/nsa-urges-sysadmins-to-replace-obsolete-tls-protocols/162814/
Infected Technology	Devices that uses TLS 1.0 and TLS 1.1 Protocol.
Recommendation	Update TLS to its latest version i.e. TLS 1.2 or TLS 1.3

For any queries/recommendations:

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