December 21, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- VMware Flaw Used to Hit Choice Targets in SolarWinds Hack
- Firefox Patches Critical Mystery Bug, Also Impacting Google Chrome
- Easy WP SMTP Security Bug Can Reveal Admin Credentials
- Microsoft Office 365 Credentials Under Attack by Fax 'Alert' Emails
- Gitpaste –12 returns to Target Linux Servers and IoT Devices
- WordPress plugin with 5 million installs has critical vulnerability
- Zebrocy's malware targeting the Golang programming language-based versions

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. VMware Flaw Used to Hit Choice Targets in SolarWinds Hack

Description

KerbsOnSecurity reported a VMware based vulnerability that allowed access to protected data and federated authentication abuse that was used to attack high-value targets by the SolarWinds hackers. The U.S. National Security Agency (NSA) also reported a software flaw in VMware on December 7th stating that the Russian hackers used this vulnerability to impersonate legitimate users. For the exploitation to occur, the hackers were required to be on the target's internal network. VMware released a software update to plug the security hole on December 3rd.

Source	https://www.crn.com/news/security/vmware-flaw-used-to-hit-choice-targets-in-solarwinds-hack-report
Infected Technology	VMware Identity Manager
Recommendation	Install the software as soon as possible.

2. Firefox Patches Critical Mystery Bug, Also Impacting Google Chrome

Description

A Mozilla Foundation update to the Firefox web browser, released Tuesday, tackles one critical vulnerability and six high-severity flaws. The update released as Firefox version 84, is also billed by Mozilla Firefox as boosting the browser's performance and adding native support for macOS hardware running on its own Apple processors. The vulnerability was introduced due to a flaw in the JavaScript component called BigInt that "could have caused uninitialized memory to be exposed. The similar vulnerability was also seen in Google, which is known as "uninitialized-use" bug that impacts upon Chrome's V8 JavaScript engine.

Source	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16042
Infected Technology	Mozilla Firefox, Google Chrome
CVE_ID	CVE-2020-16042
Recommendation	Update Firefox and Google Chrome to its latest version.

3. Easy WP SMTP Security Bug Can Reveal Admin Credentials

Description

According to the researchers, a WordPress plugin namely Easy WP SMTP, which is used for email management and is installed by more than 500,000 users, has a vulnerability that could open the site up to takeover. Easy WP SMTP allows users to configure and send all outgoing emails via a SMTP server, so that they don't end up in the recipient's junk/spam folder. Version 1.4.2 and below contains a flaw in the debug file that is exposed because of a fundamental error in how the plugin maintains a folder. The vulnerability allows an unauthenticated user to reset the admin password, which would enable the hacker to take complete control of the website.

Source	https://wordpress.org/plugins/easy-wp-smtp/
Infected Technology	Websites that have WordPress plugin Easy WP SMTP version < 1.4.2 installed.
Recommendation	Consider using another plugin for email management until patch is available.

4. Microsoft Office 365 Credentials Under Attack by Fax 'Alert' Emails

Description

A coordinated phishing attack targeted "numerous" enterprise organizations by sending a phishing mail email from compromised accounts with the aim of stealing their office 365 credentials. The widespread use of hundreds of compromised accounts and never-seen-before URLs indicate the campaign is designed to bypass traditional threat intelligence solutions accustomed to permitting known but compromised accounts into the inbox. The attack starts with a lure convincing email recipient that they received a document. The email impersonates business like eFax, which is an internet fax service making easy to receive faxes via email or online.

Source	https://abnormalsecurity.com/blog/spear-phishing-campaign-targets-enterprises/
Infected Technology	Microsoft365
CVE_ID	CVE-2020-4006
Recommendation	Do not open any eFax in mail whose interface looks similar to the one shown in the source.

5. Gitpaste –12 returns to Target Linux Servers and IoT Devices

Description

A wormable botnet that spreads from GitHub and Pastebin has returned. The main focus of this botnet is to ***install cryptocurrency miners and backdoors*** with expanded capabilities to compromise web applications, IP cameras and routers. The attacks use payloads from different GitHub repository which contains Linux crypto-miner ('ls') file with a list of passwords for brute-forcing and local privilege escalation exploits for x86_64 Linux systems. The worm conducts a series of attacks targeting web applications, IP cameras, routers and more, compromising 31 known vulnerabilities.

Source	https://blogs.juniper.net/en-us/threat-research/gitpaste-12
Infected Technology	F5 Big-IP Traffic Management User Interface, Pi-hole Web, Tenda AC15 AC1900, vBulletin and FUEL CMS
CVE	CVE-2020-5902, CVE-2020-8816, CVE-2020-10987, CVE-2020-17496 and CVE-2020-17463

6. WordPress plugin with 5 million installs has critical vulnerability

Description

A WordPress plugin, Contact Form 7, has disclosed a critical file upload vulnerability and issued a patch. This plugin has over 5 million active installs. It was a critical vulnerability because the attacker can upload a crafted file with arbitrary code on the vulnerable server. In the vulnerable version, the plugin does not remove special characters from the uploaded file name. The attacker could be able to upload a filename containing double-extensions which are separated by non-printable or special characters. The server would parse the filename until the first extension and discard the second one due to a separator hence, the attacker was able to execute arbitrary code on the server.

Source	https://www.getastra.com/blog/911/plugin-exploit/contact-form-7-unrestricted-file-upload-vulnerability/
Infected Technology	WordPress websites that have Contact Form 7 plugin.
Recommendation	Urgent update the plugin from patched version 5.3.2

7. Zebrocy's malware targeting the Golang programming language-based versions

Description

Researchers at Intezer have analyzed the latest versions of Zebrocy and discovered that the malware operators, APT28, have chosen the Golang language instead of any earlier used programming languages, such as Delphi, AutoIT, C++, C#, Delphi, and VB.NET. In his research, he observed a VHD file containing a PDF document and an executable file masquerading as a Microsoft Word document, contains the Zebrocy malware. The use of a VHD file is to hide the malware successfully which can trick the antivirus search engines from detecting the generic malware. He also claims that for distribution of this version, the threat actors are using COVID-19 vaccine-themed phishing lures embedded with malware-laden documents about Sinopharm International Corporation which can lead the social life and organization in danger.

Source	https://www.intezer.com/blog/research/russian-apt-uses-covid-19-lures-to-deliver-zebrocy/
Infected Technology	Golang, Delphi, C++, c#, VB.NET
Recommendation	Use defense-in-depth strategies for prevention of such threats.

8. Spotify security vulnerability exposed personal data to business partners

Description

Spotify said it had "contained and remediated" the data breach after discovering a security vulnerability in its system that revealed users account registration information to the third parties. Exposed data may have included email addresses, display names, passwords, gender, and date of birth, said the music streaming giant. The digital media service said this data was visible to certain business partners of Spotify but insisted that the incident did not make this information publicly accessible. However, the platform urged users "to change the passwords of all other online accounts for which you use the same email address and password" and alert them to any suspicious activity on their Spotify account.

Source	https://portswigger.net/daily-swig/spotify-security-vulnerability-exposed-personal-data-to-business-partners?&web_view=true
Infected Technology	Spotify
Recommendation	Change the user credentials immediately

9. Google claims XS-leaks attacks to be the most challenging issues for web applications and security researchers

Description

A recent article from Google revealed that attackers are increasingly leveraging a specific class of vulnerabilities derived from side-channels built into the web platform, to extract sensitive data out of any web application. Dubbed cross-site leaks known as XS-Leaks an attacker can use the existing side-channels on the web to leak sensitive information about the users from other web applications, such as details about their local environment or their internal networks. XS-Leaks takes advantage of the web's core principle of composability. It allows websites to interact with each other and abuse legitimate mechanisms to infer information about the user. To promote a better understanding of XS-Leaks google has also launched a XS-leaks wiki which main aim is to improve the state of web security posture and provide actionable guidance to assist developers in the adoption of new browser security features.

Source	https://security.googleblog.com/2020/12/fostering-research-on-new-web-security.html
Infected Technology	Web Applications
Recommendation	Use security Features such as: • Fetch Metadata Request Headers • Cross-Origin Opener Policy • Cross-Origin Resource Policy • SameSite cookies

10. 4 critical vulnerability found in valve steam can lead the attacker to steal sensitive data and remotely control target's system

Description

An IT security researcher at Checkpoint identified several critical vulnerabilities in Game Networking Socket (GNS) library that would allow attackers to hack and take over hundreds of thousands of computers remotely. The worst part is that attackers could do that without tricking users into clicking on a link or sending a phishing email to steal their Steam login credentials. Simply put the user would be affected by merely logging onto the game. Moreover, an attacker could not only remotely steal the personal data of the victim including login credentials they could also disrupt the Valve game server, crash the opponent's game client, and execute arbitrary code against 3rd party game server.

Source	https://research.checkpoint.com/2020/game-on-finding-vulnerabilities-in-valves-steam-sockets/
Infected Technology	Valve Steam, Steam Socket
CVE_ID	CVE-2020-6016, CVE-2020-6019
Recommendation	Update the library

11. PgMiner botnet attacks weakly secured PostgreSQL databases

Description

Security researchers have discovered this week a botnet operation that targets PostgreSQL databases to install a cryptocurrency miner known as Pgminer. According to researchers at Palo Alto Networks, the botnet operates by performing brute-force attacks against internet-accessible PostgreSQL database which randomly picks a public network range (e.g., 18.xxx.xxx.xxx) and then iterates through all IP addresses part of that range, searching for systems that have the PostgreSQL port (port 5432) exposed online if PgMiner finds an active PostgreSQL system, the botnet moves from the scanning phase to its brute-force phase, where it shuffles through a long list of passwords in an attempt to guess the credentials for "postgres," the default PostgreSQL account. If PostgreSQL database owners have forgotten to disable this user or have forgotten to change its passwords, the hackers access the database and use the PostgreSQL copy from program feature to escalate their access from the database app to the underlying server and take over the entire OS afterwards the PgMiner crew deploys a coin-mining application and attempt to mine as much Monero cryptocurrency before they get detected.

Source	https://unit42.paloaltonetworks.com/pgminer-postgresql-cryptocurrency-mining-botnet/
Infected Technology	PostgreSQL Databases
Recommendation	• Change the PostgreSQL default username and password • Close the 5432 port if not used

For any queries/recommendations:

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