QUALYSEC
BEYOND CYBERSECURITY

2023

MAY 1ST WEEK

CYBER SECURITY NEWS

CONTACT US

www.qualysec.com
865 866 3664
contact@qualysec.com

Warning! TP-Link, Apache, and Oracle Vulnerabilities Actively Exploited in Wild

CISA recently included three actively exploited vulnerabilities in the wild in its KEV (Known Exploited Vulnerabilities) catalog.

The three actively exploited vulnerabilities are detected in:-

- TP-Link
- Apache
- Oracle

Here below we have mentioned the vulnerabilities:-

- CVE-2023-1389
- CVE-2021-45046
- CVE-2023-21839

Federal Government agencies and enterprises face a significant number of risks as a result of vulnerabilities of this type, which are prone to be exploited by threat actors.

CVE-2021-45046, it's a remote code execution vulnerability that came to light in December 2021.

This vulnerability affects the Apache Log4j2 logging library, and it is the second flaw added to the KEV catalog.

While there is no clear indication of how the vulnerability is being exploited, GreyNoise's data suggests that in the past 30 days, 74 unique IP addresses attempted to exploit it.

Source : https://cybersecuritynews.com/warning-tp-link-apache-and-oracle-vulnerabilities/

T-Mobile Hacked – Over 37M Sensitive Data Exposed

T-Mobile claims it discovered that threat actors had gained limited access to information from a few accounts. This is the year's second instance of a data leak.

Hackers had had hundreds of customers' personal information for over a month, beginning in late February 2023.

"In March 2023, the measures we have in place to alert us to unauthorized activity worked as designed and we were able to determine that a bad actor gained access to limited information from a small number of T-Mobile accounts between late February and March 2023," in data breach notification letters issued to affected people, the company made this statement.

In contrast to T-Mobile's past data breaches, the most recent of which affected 37 million users, reports say this incident only affected 836 customers.

What Details Were Involved?

The exposed personally identifiable information comprises more than enough information for identity theft, according to T-Mobile. However, the threat actors did not obtain access to call logs or the affected people's personal financial account information.

Source : https://cybersecuritynews.com/t-mobile-hacked-data-exposed/

APT41's PowerShell Backdoor Let Hackers Download & Upload Files From Windows

Researchers from Threatmon uncovered a targetted PowerShell backdoor malware attack from APT41 that bypasses the detections and allows threat actors to execute commands, download and upload files, and gather sensitive information from compromised Windows systems.

Since 2012, the Chinese cyber espionage group APT41 (aka Wicked Panda) has used advanced tactics, techniques, and procedures (TTPs). They use custom-built malware and tools such as a PowerShell backdoor in their malicious arsenal.

Microsoft Windows comprises the built-in scripting language PowerShell, and it can manage the system configurations and automate administrative tasks.

"By exploiting this functionality, APT41's PowerShell backdoor circumvents conventional security measures, enabling it to infiltrate target systems, Alp Cihangir ASLAN & Seyit SIGIRCI Malware Analyst's from Threat Intelligence Firm, ThreatMon Reported to Cyber Security News. "The group is also known for using a wide range of sophisticated tools and techniques, including custom malware, supply chain attacks, and the exploitation of vulnerabilities in software and hardware."

Source : https://cybersecuritynews.com/apt41s-powershell-backdoor/

Thousands of Apache Superset Servers Open to RCE Attacks

Cybersecurity analysts at Horizon3 detected that thousands of Apache Superset servers are exposed to RCE attacks at default configurations.

This could allow the threat actors to perform the following illicit activities:-

- Access data
- Modify data
- Harvest credentials
- Execute commands

Apache Superset is an open-source tool that is used for:-

- Data visualization
- Data exploration

Initially, this tool was developed for Airbnb, but in 2021, it became a top-level project at the Apache Software Foundation.

Technical Analysis

Attackers could take advantage of the default Flask Secret Key utilized by Apache Superset for signing authentication session cookies to create fake session cookies.

Consequently, servers that haven't altered the key may be susceptible to unauthorized access with elevated privileges.

Source : https://cybersecuritynews.com/thousands-of-apache-superset-servers-open-to-rce-attacks/

Ex-Uber CSO Avoids Prison Time for Concealing Data Breach

On Wednesday, an ex-Uber CSO was found guilty of federal charges related to payments he secretly approved to hackers who broke into the ride-hailing company in 2016

For concealing the breach from the Federal Trade Commission, which was looking into Uber's privacy measures at the time, Joe Sullivan was found guilty of obstructing justice and intentionally concealing a felony.

The Sentencing

A federal jury found Sullivan guilty on two counts stemming from his attempt to hide a security breach at Uber in 2016, during which hackers obtained the personal information of 57 million users and 600,000 Uber drivers.

After a 2014 hack resulted in the exposure of the names and driver's license information of 50,000 users, Uber was ordered by the Federal Trade Commission to notify all breaches.

Instead, Sullivan gave the two hackers a $100,000 payment and forced them to sign nondisclosure agreements without telling the FTC. He described the payments as a bug bounty to defend them.

Source : https://cybersecuritynews.com/ex-uber-cso-avoids-prison-time/

Over 2 Million WordPress Websites Exposed to XSS Attacks

Patchstack security researchers recently warned that 'Advanced Custom Fields' and 'Advanced Custom Fields Pro' WordPress plugins are at risk of cross-site scripting attacks (XSS).

These WP plugins, installed on millions of websites, may be vulnerable to security breaches.

The 'Advanced Custom Fields' and 'Advanced Custom Fields Pro' plugins are renowned custom field builders for WordPress and have accumulated a significant user base, with over 2 million active installations.

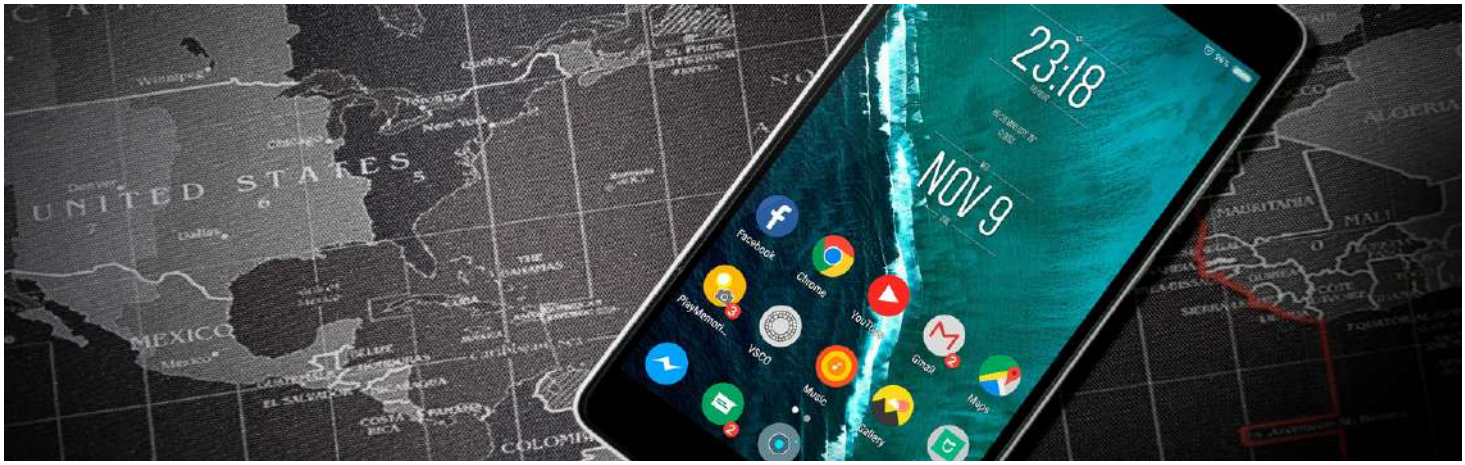
On May 2, 2023, a severe reflected XSS vulnerability was identified by Rafie Muhammad, a researcher at Patchstack, and the vulnerability has been tracked as "CVE-2023-30777."

Vulnerability in Advanced Custom Fields

XSS vulnerabilities provide a gateway for malevolent actors to inject harmful scripts onto websites accessed by unsuspecting users.

In short, this enables the code to run within the visitor's browser and compromise their security. According to Patchstack, an unauthenticated adversary could exploit the XSS vulnerability to steal confidential data and even elevate their privileges on a compromised WordPress site.

Source : https://cybersecuritynews.com/over-2-million-wordpress-websites-exposed-to-xss-attacks/



New Android Malware on Google Play Installed Over 620,000 Times

A recently discovered Android subscription malware called 'Fleckpe' has surfaced on Google Play Store. This insidious malware disguises itself as an authentic application and has already been downloaded by more than 620,000 users into downloading it.

According to Kaspersky, Fleckpe is the latest addition to the notorious malware family that illegitimately charges users by enrolling them in premium services.

This new malware has joined the ranks of other malicious Android programs, including Jocker and Harly, which exploit unsuspecting victims for financial gain.

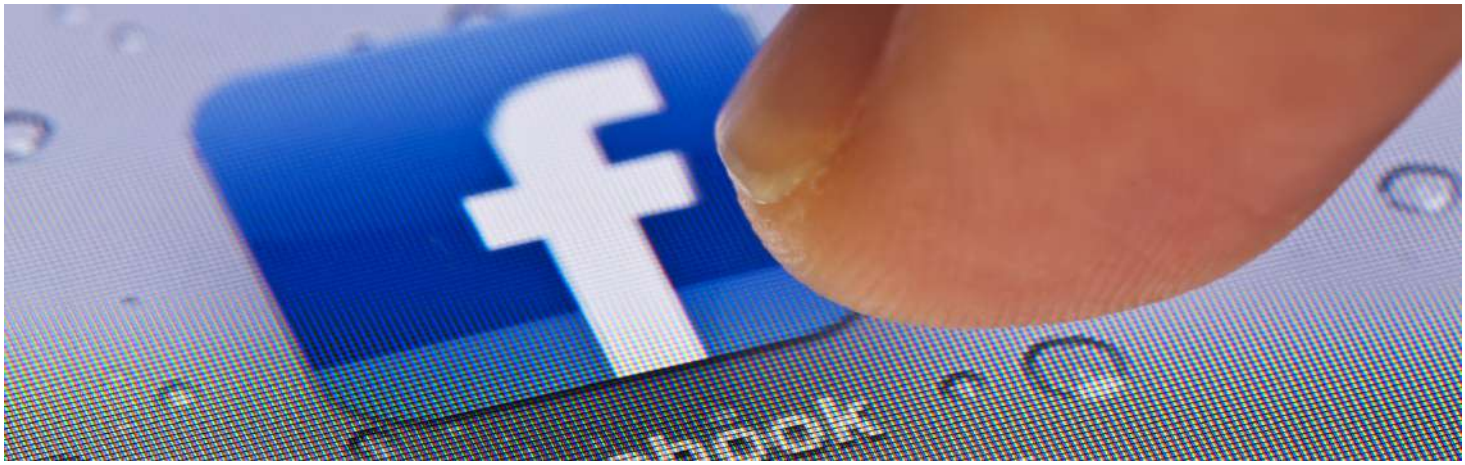
Unauthorized subscriptions generate revenue for threat actors, who earn a portion of premium services' monthly or one-time subscription fees.

Malware on Google Play

Moreover, the cybersecurity experts at Kaspersky Lab asserted that the malware has been operating since last year, but its detection and documentation only occurred recently.

Moreover, they also recommended installing a reputed antivirus to detect and protect against this type of Trojan to mitigate such infections and financial losses.

Source : https://cybersecuritynews.com/new-android-malware-google-play/



Facebook Take Down ChatGPT-themed Malware Attacks That Stole FB Accounts

NodeStealer, a newly discovered malware on Meta, was identified by Facebook as stealing browser cookies.

Due to this vulnerability, threat actors can obtain illicit entry into various accounts on the platform, including Gmail and Outlook. Threat actors are increasingly adopting the tactic of capturing cookies that hold valid user session tokens.

It enables them to bypass two-factor authentication measures; hijack accounts without stealing credentials or interacting with targets.

Facebook's security team detected NodeStealer at an early stage of its distribution campaign, just within two weeks of its initial release.

The company swiftly addressed the situation and assisted affected users in recovering their accounts, ultimately disrupting the operation.

Ducktail Malware in Focus

Over multiple years, Facebook's security team monitored and obstructed various versions of Ducktail originating from Vietnam, which have adapted in response to measures implemented by Meta and its counterparts in the industry.

Source : https://cybersecuritynews.com/facebook-chatgp-themed-attacks/

VirusTotal New “Crowdsourced YARA Hub” Let Security Researchers Filter Yara Rules

VirusTotal has introduced a Crowdsourced YARA Hub to overcome this hurdle, letting users find and filter existing rules, track a new rule, and export rules to LiveHunt or Retrohunt with a Single Click.

YARA (Yet Another Ridiculous Acronym) rules are malware detection patterns that can help strategize a targeted attack or a threat. VirusTotal is one of the largest platforms of Threat Intelligence utilized by security researchers.

VirusTotal offers both Livehunt (Streaming of files analyzed by VirusTotal and get notified when there is a match) and Retrohunt (scanning up to 12 months-old files sent to VirusTotal by user-created YARA rules).

VirusTotal has several contributors worldwide who submit various YARA rules that can identify and classify samples. Due to the increasingly large crowdsourcing of rules, Finding and keeping track of all the rules is challenging.

YARA Hub does not list private Livehunt or Retrohunt rulesets. Instead, it lists all the community YARA rules in the context of files currently being processed by VirusTotal. The YARA hub is found under “Livehunt” in VirusTotal.

Source : https://cybersecuritynews.com/crowdsourced-yara-hub/

Hacker Groups Adding New Double DLL Sideloading Technique to Evade Detection

The cybersecurity security researchers at Sophos recently detected the “Dragon Breath” APT group (aka Golden Eye Dog, APT-Q-27) using complex DLL sideloading variations to avoid detection.

The APT group deploys a new attack vector that utilizes clean applications like Telegram to malicious malware loader DLLs and sideloads second-stage payloads.

DLL Sideloading

APT actors use BlackSEO or malvertizing techniques to promote malicious versions of Telegram, LetsVPN, or WhatsApp apps that are localized for Chinese users as bait to infect victims on Android, iOS, or Windows platforms.

According to Sophos report, this campaign is primarily targeting Chinese-speaking Windows users in the following countries:-

- China
- Japan
- Taiwan
- Singapore
- Hong Kong
- The Philippines

Source : https://cybersecuritynews.com/double-dll-sideloading-technique-to-evade-detection/

“It is crucial for users to exercise caution when receiving spam emails or to visit phishing websites and to verify the source before downloading any applications”, concludes the researchers.

It's a fact that cybercrime is on the rise and it's more important than ever to protect your business from cyber threats.

But the good news is that you don't have to navigate the complex world of cybersecurity alone. Our team of experts is here to help you cyber security testing services need to protect your application or business.

Don't wait for a cyber attack to happen. Contact us now to learn more about how we can help secure your business and give you peace of mind.

Contact now and protect your business with our expert cyber security services.

CONTACT US AT