CERT-PH Cybersecurity Threat Feeds

Issue Date	March 30, 2021
TLP: White	

Summary

The latest cyber threat topics gathered from the web and analyzed by the CERT-PH research team over the last 24 hours that may impact the Philippine government and cyberspace:

- Experts Found Two Flaws in Facebook for WordPress Plugin
- New Purple Fox Version Includes Rootkit And Implements Wormable Propagation
- Critical Netmask Networking Bug Impacts Thousands Of Applications
- PHP's Git Server Breached to Insert Secret Backdoor

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

Experts Found Two Flaws in Facebook for WordPress Plugin

2021.03.28 | Source(s): Security Affairs, Security Week

Analysis:

Researchers discovered two vulnerabilities in the Facebook for Wordpress plugin. Previously known as Official Facebook Pixel, the plugin allows administrators to capture the actions people take while interacting with their page including Lead, ViewContent, AddToCart, InitiateCheckout and Purchase events. The flaw is a PHP object injection with POP chain that could be exploited by an unauthenticated attacker to access a site's secret and keys and exploit a deserialization weakness to achieve remote code execution. In addition, security researchers discovered a Cross-Site Request Forgery to Stored Cross-Site Scripting vulnerability which could be exploited by an attacker to update the plugin's settings and steal metric data for a site and also inject malicious JavaScript code into the setting values. The code could then be used to inject malicious backdoors into theme files or create new administrative user accounts that could be used to take over the site.

Read more:

[https://securityaffairs[.]co/wordpress/116063/social-networks/facebook-wordpress-plugin-attacks.html]
[https://www.securityweek[.]com/severe-flaws-official-facebook-wordpress-plugin]

New Purple Fox Version Includes Rootkit and Implements Wormable Propagation

2021.03.29 | Source(s): Security Affairs

Analysis:

Security researchers have spotted a new variant of the Purple Fox Windows malware that implements worm-like propagation capabilities. The previous versions of the malware were infecting machines by using exploit kits and phishing emails, while the new variant is targeting Windows machines exposed online through SMB password brute force. According to researchers, once the malware infected a system, the malware blocks multiple ports (445, 139 and 135) to prevent the infected machine from being reinfected or targeted by other attackers. The malware attempts to spread by generating IP ranges and scanning them on port 445, then will try to authenticate to SMB by performing brute attacks or by trying to establish a null session. Moreover, once the rootkit is loaded, the installer will reboot the machine in order to rename the malware DLL into a system DLL file that will be executed on boot and once the machine is restarted, the malware will be executed as well. After it's execution, the malware will start its propagation process.

Read more:

[https://securityaffairs[.]co/wordpress/116070/malware/purple-fox-rootkit-version.html]

Critical Netmask Networking Bug Impacts Thousands of Applications

2021.03.28 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts discovered a critical networking vulnerability in the popular npm library Netmask. Tracked as CVE-2021-28918, the vulnerability concerns how Netmask handles mixed-format IP addresses, or more specifically when a decimal IPv4 address contains a leading zero. According to researchers, when an attacker is able to influence the IP address input being parsed by the application, the bug can give rise to various vulnerabilities. This bug can also be exploited for Remote File Inclusion (RFI) should an attacker craft an IP address that looks private to netmask, because of the way netmask converts all IPv4 parts (octets) to decimal format, but is evaluated as public by other components. In addition, this flaw could also be exploited to bypass IP-based Access Control Lists (ACLs) and Server-Side Request Forgery (SSRF) bypasses

Read more:

[https://www.bleepingcomputer[.]com/news/security/critical-netmask-networking-bug-impacts-thousands-of-applications/]

PHP’s Git Server Breached to Insert Secret Backdoor

2021.03.29 | Source(s): Security Affairs, Threatpost

Analysis:

Unknown attackers hacked the official Git server of the PHP programming language and pushed unauthorized updates to insert a backdoor into the source code. The threat actors pushed two commits to the “php-src” repository hosted on the git.php.net server, they used the accounts of Rasmus Lerdorf, the PHP’s author, and Jetbrains developer Nikita Popov. According to the experts, they believe that attackers have compromised the git.php.net server. The analysis of malicious code revealed the presence of a string “Zerodium,” which is the name of one of the most popular zero-day brokers. In response, PHP is moving its servers to GitHub, making them canonical.

Read more:

[https://securityaffairs[.]co/wordpress/116088/hacking/php-git-server-hack.html]
[https://threatpost[.]com/php-infiltrated-backdoor-malware/165061/]

CERT-PH Recommendations:

- QNAP users are urged to secure their NAS devices by changing the default access port number, using strong passwords for their accounts, enabling password policies, and disabling the admin account targeted in these ongoing attacks.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Facebook for WordPress Plugin** - version 3.0.5 or later
  - **Netmask NPM Library** - version 2.0.0 or later
- Agencies must protect their assets and perimeter by minimizing the point of entry that an unwanted attacker might take. Thus, actions must be taken such as:
  - Closing misconfigured and/or unused ports that are accessible in the public internet.
  - Regularly monitoring and patching of systems, software application, and devices.
  - Educating employees regarding cyber hygiene and cybersecurity best practices.

Critical	*The information stated is deemed to be crucial to organizations and can significantly shift security concerns and issues based on following events.*
Urgent	*The information stated needs to be addressed timely, which may require immediate attention and/or prompt action.*
Information	*The information stated is good to know knowledge that provides awareness and understanding to the topic.*