CERT-PH Cybersecurity Threat Feeds

Issue Date	March 26, 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:

- OpenSSL Project Fixed Two High-severity Flaws
- Severe Vulnerabilities Patched in Facebook For WordPress Plugin
- Active Exploits Hit WordPress Sites Vulnerable to Thrive Themes Flaws
- QNAP Warns Of Ongoing Brute-force Attacks Against NAS Devices

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

OpenSSL Project Fixed Two High-severity Flaws

2021.03.25 | Source(s): Bleeping Computer, Security Affairs

Analysis:

The OpenSSL Project addresses two high-severity vulnerabilities, including one related to verifying a certificate chain and one that can trigger a DoS condition. Tracked as CVE-2021-3449, the vulnerability could be exploited to trigger a DoS condition by sending a specially crafted renegotiation ClientHello message from a client. This affects servers running OpenSSL 1.1.1 versions with TLS 1.2 and renegotiation enabled. The second vulnerability, tracked as CVE-2021-3450, is related to the verification of a certificate chain when using the X509_V_FLAG_X509_STRICT flag. According to researchers, an error in the implementation of this check meant that the result of a previous check to confirm that certificates in the chain are valid CA certificates was overwritten. This effectively bypasses the check that non-CA certificates must not be able to issue other certificates

Read more:

[https://securityaffairs[.]co/wordpress/115968/security/openssl-flaws-2.html]
[https://www.bleepingcomputer[.]com/news/security/openssl-fixes-severe-dos-certificate-validation-vulnerabilities/]

Severe Vulnerabilities Patched in Facebook For WordPress Plugin

2021.03.25 | Source(s): ZDNet

Analysis:

Cybersecurity researchers discovered a bug that impacts Facebook for Wordpress, also known as Official Facebook Pixel. The plugin is used to capture user actions when they visit a page and to monitor site traffic. The flaw detected is a PHP Object injection vulnerability that exists in the run_action() function of the software. An attacker could supply the plugin with PHP objects for malicious purposes and go so far as to upload files to a vulnerable website and achieve Remote Code Execution (RCE). The second flaw is a cross-site request forgery security flaw vulnerability that could be used by an attacker to update the plugin's settings to point to their own Facebook Pixel console and steal metric data for a site. In addition, malicious Javascript could be used to create backdoors in themes or create new admin accounts for hijacking entire websites.

Read more:

[https://www.zdnet[.]com/article/severe-vulnerabilities-patched-in-facebook-for-wordpress-plugin/]

Active Exploits Hit WordPress Sites Vulnerable to Thrive Themes Flaws

2021.03.24 | Source(s): Threatpost

Analysis:

Thrive Themes recently patched vulnerabilities in its WordPress plugins and legacy Themes that threat actors are actively exploiting in the wild. The most critical among the flaws exists in Thrive Themes Legacy Themes which has the ability to automatically compress images during uploads, however this functionality was insecurely implemented. According to security researchers, by supplying a crafted request in combination with data inserted using the Option Update vulnerability, it is possible to use this endpoint to retrieve malicious code from a remote URL and overwrite an existing file on the site with it or create a new file. This includes executable PHP files that contain malicious code.

Read more:
[https://threatpost[.]com/active-exploits-wordpress-sites-thrive-themes/165013/]

QNAP Warns Of Ongoing Brute-force Attacks Against NAS Devices

2021.03.24 | Source(s): Security Affairs

Analysis:

QNAP warns customers of ongoing attacks targeting QNAP NAS (network-attached storage) devices. Threat actors use automated tools to login into Internet-exposed NAS devices using passwords generated on the spot or from lists of previously compromised credentials. QNAP has received multiple user reports of hackers attempting to log in to QNAP devices using brute-force attacks, where hackers would try every possible password combination of a QNAP device user account. After guessing the right combination, threat actors get full access to the targeted device, allowing them to gain access to and steal sensitive documents or deploy malware.

Read more:
[https://www.bleepingcomputer[.]com/news/security/qnap-warns-of-ongoing-brute-force-attacks-against-nas-devices/]

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:
    - **OpenSSL Project** - version 1.1.1k or later
    - **QNAP NAS QTS** - latest version
    - **Facebook for WordPress** - version 3.0.5 or later
- aAgencies 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.*