CERT-PH Cybersecurity Threat Feeds

Issue Date	March 22, 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:

- Critical F5 BIG-IP Vulnerability Now Targeted In Ongoing Attacks
- Hacking Group Used 11 Zero-days to Attack Windows, iOS, Android users
- Millions of Sites Could Be Hacked Due to Flaws in Popular WordPress Plugins
- Critical RCE Flaw Reported in MyBB Forum

- CRITICAL
- URGENT
- INFORMATION

Description

Critical F5 BIG-IP Vulnerability Now Targeted In Ongoing Attacks

2021.03.19 | Source(s): Bleeping Computer, Security Affairs, Threatpost

Analysis:

Cybersecurity researchers detected several exploitation of the recently patched critical vulnerability in F5 BIG-IP and BIG-IQ networking devices. Tracked as CVE-2021-22986, the vulnerability is an unauthenticated remote command execution (RCE) flaw with a severity rating of 9.8 out of 10. Successful exploitation could lead to full system compromise, including lateral movement to the internal network and interception of controller application traffic. The vulnerability could be exploited by unauthenticated attackers with network access to the iControl REST interface, through the BIG-IP management interface and self IP addresses, to execute arbitrary system commands, create or delete files, and disable services.

Read more:

[https://www.bleepingcomputer[.]com/news/security/critical-f5-big-ip-vulnerability-now-targeted-in-ongoing-attacks/]
[https://securityaffairs[.]co/wordpress/115760/hacking/f5-big-ip-attacks-cve-2021-22986.html]
[https://threatpost[.]com/critical-f5-big-ip-flaw-now-under-active-attack/164940/]

Hacking Group Used 11 Zero-days to Attack Windows, iOS, Android users

2021.03.20 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts discovered a group of hackers that used 11 zero-days in attacks targeting Windows, iOS and Android users within a single year. The threat actors behind these attacks ran two separate campaigns in February and October 2020. The attackers used a couple of dozen websites hosting two exploit servers, each of them targeting iOS and Windows or Android users. According to the researchers, after initial fingerprinting, an iframe was injected into the website pointing to one of the two exploit servers. In total, cybersecurity experts found one full exploit chain targeting fully patched Windows 10 using Google Chrome, two partial chains targeting 2 different fully patched Android services running Android 10 using Google Chrome and Samsung Browser and several RCE exploits for iOS 11-13 and a privilege escalation exploit for iOS 13, with the exploited bugs present up to iOS 14.1.

Read more:

[https://www.bleepingcomputer[.]com/news/security/hacking-group-used-11-zero-days-to-attack-windows-ios-android-users/]

Millions of Sites Could Be Hacked Due to Flaws in Popular WordPress Plugins

2021.03.19 | Source(s): Security Affairs

Analysis:

Security researchers disclosed vulnerabilities in Elementor and WP Super Cache WordPress plugins that could be exploited to run arbitrary code and take over a website under certain circumstances. Multiple stored cross-site scripting (XSS) flaws exist in the Elementor plugin, collectively received a CVSS score of 6.4. The flaws were due to the lack of server-side validation for HTML tags in Elementor elements that allows any users to add executable JavaScripts to a post or page via a crafted request. On the other hand, a flaw in the WP Super Cache plugin could also be exploited by attackers to execute malicious code, potentially resulting in the site takeover.

Read more:

[https://securityaffairs[.]co/wordpress/115750/hacking/wordpress-plugins-flaws.html]

Critical RCE Flaw Reported in MyBB Forum

2021.03.18 | Source(s): The Hacker News

Analysis:

Cybersecurity researchers discovered a pair of critical vulnerabilities in a popular bulletin board software called MyBB that could have been chained together to achieve remote code execution (RCE) without the need for prior access to a privileged account. Tracked as CVE-2021-27889, a nested auto URL persistent XSS vulnerability that stems from how MyBB parses messages containing UPLs during the rendering process, thus enabling any unprivileged forum user to embed stored XSS payloads into threads, posts and even private messages. The second flaw, tracked as CVE-2021-27890, an SQL injection in a forum's theme manager that could result in an authenticated RCE. A successful exploitation occurs when a forum administrator with the "Can manage themes?" permission imports a maliciously crafted theme, or a user, for whom the theme has been set, visits a forum page.

Read more:

[https://thehackernews[.]com/2021/03/critical-rce-flaw-reported-in-mybb.html]

CERT-PH Recommendations:

- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **F5 BIG-IP and BIG-IQ** - latest version
  - **Google Chrome (Windows and Mobile)** - latest version
  - **iOS** - latest version
  - **Elementor** - version 3.1.4
  - **WP Super Cache** - version 1.7.2
  - **MyBB** - version 1.8.26 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.*