CERT-PH Cybersecurity Threat Feeds

Issue Date	March 12, 2021
TLP: GREEN	

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:

- Android Apps on Google Play Caught Distributing AlienBot Banker and MRAT Malware
- Flaw in The Plus Addons For Elementor WordPress Plugin Allows Sites Takeover
- Microsoft's March Patch Tuesday Fixes 14 Critical Flaws
- F5 Addresses Critical Vulnerabilities in BIG-IP and BIG-IQ

- CRITICAL
- URGENT
- INFORMATION

Description

Android Apps on Google Play Caught Distributing AlienBot Banker and MRAT Malware

2021.03.09 | Source(s): The Hacker News

Analysis:

Cybersecurity experts discovered a new malware dropper contained in 9 Android apps distributed via Google Play Store that deploys a second stage malware capable of gaining intrusive access to the financial accounts of victims as well as full control of their device. Dubbed as Clast82, the dropper utilizes a series of techniques to avoid detection by Google Play Protect detection, completes the evaluation period successfully and changes the payload dropped from a non-malicious payload to the AlienBot Banker and MRAT. Clast82 utilizes Firebase as a platform for command and control communication and makes use of GitHub to download the malicious payloads, in addition to leveraging legitimate and known open-source Android applications to insert the Dropper functionality.

Read more:

[https://thehackernews[.]com/2021/03/9-android-apps-on-google-play-caught.html]

Flaw in The Plus Addons For Elementor WordPress Plugin Allows Sites Takeover

2021.03.10 | Source(s): Security Affairs

Analysis:

Cybersecurity researchers from the Wordfence team found a critical vulnerability in The Plus Addons for Elementor WordPress plugin that could be exploited by attackers to gain administrative privileges to a website and take over it. The Plus Addons for Elementor allows users to add several widgets to the popular WordPress website builder Elementor. The vulnerability exists in one of the widgets that the plugin allows to add, it allows designers and developers to insert user login and registration forms to Elementor pages. In addition the flaw allows attackers to create new administrative user accounts on vulnerable sites when the user registration is enabled, and log in as other administrative users.

Read more:

[https://securityaffairs[.]co/wordpress/115451/hacking/the-plus-addons-for-elementor-wordpress-flaw.html]

Microsoft's March Patch Tuesday Fixes 14 Critical Flaws

2021.03.10 | Source(s): Security Affairs

Analysis:

Microsoft's March Patch Tuesday security updates address 89 vulnerabilities in its products, including Microsoft Windows components, Azure and Azure DevOps, Azure Sphere, Internet Explorer and Edge (EdgeHTML), Exchange Server, Office and Office Services and Web Apps, SharePoint Server, Visual Studio, and Windows Hyper-V. Tracked as CVE-2021-26411, one of the most severe flaws addressed is an Internet

Explorer memory corruption bug. The flaw could allow attackers to run arbitrary code on affected systems by tricking victims into viewing specially crafted HTML files. The vulnerability received a CVSS score of 8.8.

Read more:

[https://securityaffairs[.]co/wordpress/115439/security/microsofts-march-patch-tuesday-21.html]

F5 Addresses Critical Vulnerabilities in BIG-IP and BIG-IQ

2021.03.10 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Security firm F5 patches seven vulnerabilities in BIG-IP, four of which have been rated as "critical" severity. Two of which are remote code execution in iControl REST and Appliance Mode TMUI tracked as CVE-2021-22986 and CVE-2021-22987 respectively. In particular, the flaw in the Appliance Mode TMUI allows authenticated users with network access to the Configuration utility, through the BIG-IP management port, or self IP addresses, to execute arbitrary system commands, create or delete files, or disable services. Exploitation can lead to complete system compromise and breakout of Appliance mode. The other two flaws were buffer overflow in TMM and Advanced WAF/ASM tracked as CVE-2021-22991 and CVE-2021-22992, respectively.

Read more:

[https://securityaffairs[.]co/wordpress/115481/security/f5-flaws-big-ip-big-iq.html]
[https://www.bleepingcomputer[.]com/news/security/f5-urges-customers-to-patch-critical-big-ip-pre-auth-rce-bug/]

CERT-PH Recommendations:

- Users are advised to be cautious and always check the authenticity of the website before giving any private information or login credentials. Phishing attacks often use multiple redirects and unsecure connections before landing on the attacker's controlled website. If unsure of the website visited and causes to raise red flags, immediately put the website in your browser's list of locked webpages.
- For users that host a website on port 554, switch to a different port to allow visitors to continue accessing your application.
- Android users are urged to check their devices and immediately uninstall and remove the following applications:
  - **Cake VPN**
  - **Pacific VPN**
  - **eVPN**
  - **BeatPlayer**
  - **QR/Barcode Scanner MAX**
  - **Music Player**
  - **tooltipnatorlibrary**
  - **QRecorder**
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **The Plus Addons for Elementor Lite - version 4.1.7**
  - **Microsoft March 2021 Patch**
  - **BIG-IP - latest version**
- 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.*