CERT-PH Cybersecurity Threat Feeds

Issue Date	March 10, 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:

- Microsoft Office 365 Gets Protection Against Malicious XLM Macros
- Adobe Critical Code-Execution Flaws Plague Windows Users
- Samsung Fixes Critical Android Bugs In March 2021 Updates
- Apple Plugs Severe WebKit Remote Code-Execution Hole

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

Microsoft Office 365 Gets Protection Against Malicious XLM Macros

2021.03.07 | Source(s): Bleeping Computer

Analysis:

Microsoft added a XLM macro protection for Microsoft 365 customers by expanding the runtime defense provided by Office 365's integration with Antimalware Scan Interface (AMSI) to include Excel 4.0 (XLM) macro scanning. AMSI allows Windows 10 services and apps to communicate with the security products and request runtime scans of potentially dangerous data. This helps expose malicious intent even when hidden using heavy obfuscation and to detect and block malware abusing Office VBA macros and Powershell, JScript, VBScript, MSHTA/Jscript9, WMI or .NET code, regularly used to deploy malware payloads via Office document macros. According to security experts, administrators can now use the existing Microsoft 365 applications policy control to configure when both XLM and VBA macros are scanned at runtime via AMSI.

Read more:
[https://www.bleepingcomputer[.]com/news/security/microsoft-office-365-gets-protection-against-malicious-xlm-macros/]

Adobe Critical Code-Execution Flaws Plague Windows Users

2021.03.09 | Source(s): Threatpost, Bleeping Computer, ZDNet

Analysis:

Adobe issued patches for critical security vulnerabilities that if exploited, could allow for arbitrary code execution on vulnerable Windows systems. Several products were affected by the flaws including Adobe's Framemaker document processor, designed for writing and editing large or complex documents; Adobe's Connect software, used for remote web conferencing and Adobe Creative Cloud software suite for video editing. Tracked as CVE-2021-21056, the vulnerability that exists in Framemaker is an out-of-bounds read error which is a type of buffer overflow flaw where the software reads data past the end of the intended buffer which can be exploited to get secret values, such as memory addresses, that could eventually be used to achieve code execution or denial of service. In Adobe Connect, the patch fixed one critical and three important cross-site scripting (XSS) tracked as CVE-2021-21078, CVE-2021-21079, CVE-2021-21080 and CVE-2021-21081, respectively. While in Creative Cloud, a total of three vulnerabilities were fixed including two critical flaws that could enable arbitrary code execution, tracked as CVE-2021-21068 and CVE-2021-21078. While the third flaw, tracked as CVE-2021-21069, could allow an attacker to gain escalated privileges and is due to improper input validation.

Read more:
[https://threatpost[.]com/wordpress-injection-malware-campaign/164555/]

Samsung Fixes Critical Android Bugs In March 2021 Updates

2021.03.06 | Source(s): Bleeping Computer

Analysis:

Samsung released Android's March security updates to mobile devices to patch critical security vulnerabilities in the runtime, operating system, and related components. Tracked as CVE-2021-0397, one of the critical vulnerabilities fixed, resides in the Android System arising from a null pointer. The vulnerability in Android's BLuetooth Service Discovery Protocol (SDP) implementation, called Fluoride Bluetooth stack, could allow an attacker to perform remote code execution attacks via a specially crafted Bluetooth transmission.

Read more:
[https://www.bleepingcomputer[.]com/news/security/samsung-fixes-critical-android-bugs-in-march-2021-updates/]

Apple Plugs Severe WebKit Remote Code-Execution Hole

2021.03.09 | Source(s): Security Affairs, Threatpost

Analysis:

Apple has released out-of-band security patches to address a critical security flaw that affects iOS, macOS, watchOS, and Safari web browser. Tracked as CVE-2021-1844, the vulnerability could be exploited by remote threat actors to run arbitrary code on vulnerable devices by tricking users into visiting a malicious web content. The flaw receives a CVSS score of 7.7 out of 10 and is caused by a memory corruption issue in its Webkit browser engine that could be triggered to cause arbitrary code execution when processing specially crafted web content. An exploit would allow an attacker to remotely execute code and ultimately take over the system.

Read more:
[https://securityaffairs[.]co/wordpress/115423/hacking/apple-cve-2021-1844-rce.html]
[https://threatpost[.]com/apple-webkit-remote-code-execution/164595/]

CERT-PH Recommendations:

- Update any vulnerable system/applications/devices to their latest and patched versions:
  - Microsoft 365 - latest version
  - Android System - March Security Update
  - Adobe Framework - version 2020.0.2
  - Creative Cloud - version 5.4
  - Adobe Connect - version 11.2
  - iOS - version 14.4
  - iPadOS - version 14.4
  - macOS Big Sur - latest version
  - **watchOS** - version 7.3.1
- 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.*