CERT-PH Cybersecurity Threat Feeds

Issue Date	March 29, 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:

- SolarWinds Patches Critical Code Execution Bug In Orion Platform
- Apple Fixes a iOS Zero-day Vulnerability Actively Used In Attacks
- Researchers Spotted A New Advanced Android Spyware Posing As "System Update"

- CRITICAL
- URGENT
- INFORMATION

Description

SolarWinds Patches Critical Code Execution Bug In Orion Platform

2021.03.26 | Source(s): Bleeping Computer, Security Affairs

Analysis:

SolarWinds recently released security updates to address four vulnerabilities impacting the company's Orion IT monitoring platform. The most critical of these flaws is a critical JSON deserialization bug that remote attackers can exploit to execute arbitrary code through Orion Platform Action Manager's test alert actions. The second remote code execution vulnerability, rated as high severity, could allow attackers to execute arbitrary code remotely as an Administrator was addressed in the SolarWinds Orion Job Scheduler. Two more vulnerabilities were fixed, tracked as CVE-2020-5856 and CVE-2021-3109, a stored XSS in customize view and a reverse Tabnabbing and Open Redirect flaws respectively.

Read more:

[https://www.bleepingcomputer[.]com/news/security/solarwinds-patches-critical-code-execution-bug-in-orion-platform/]
[https://securityaffairs[.]co/wordpress/115983/security/solarwinds-updates-rce.html]

Apple Fixes a iOS Zero-day Vulnerability Actively Used In Attacks

2021.03.26 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Apple released security updates to address an iOS zero-day bug actively exploited in the wild and affecting iPhone, iPad, iPod, and Apple Watch devices. Tracked as CVE-2021-1879, the zero-day vulnerability exists in the Webkit browser engine and could be exploited to allow attackers to launch universal cross-site scripting attacks after tricking targets into opening maliciously crafted web content on their devices.

Read more:

[https://www.bleepingcomputer[.]com/news/security/apple-fixes-a-ios-zero-day-vulnerability-actively-used-in-attacks/]
[https://securityaffairs[.]co/wordpress/116007/security/apple-zero%e2%80%91day.html]

Researchers Spotted A New Advanced Android Spyware Posing As "System Update"

2021.03.27 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Cybersecurity experts discovered a new sophisticated Android spyware that masquerades itself as a System Update application. The malware is able to collect system data, messages, images and take over the infected Android devices, it could allow operators to record audio and phone calls, take photos, review browser history, access WhatsApp messages, and more. The spyware can only be installed as a 'System Update' app via third-party Android app stores as it was never available on Google's Play Store. According to researchers, once downloaded the malicious app from a third-party store and installed it, the spyware registers itself with a Firebase command-and-control (C2) server

with information such as the presence of WhatsApp, battery percentage, and storage stats. The malware exfiltration data from the infected devices in the form of an encrypted ZIP file.

Read more:

[https://securityaffairs[.]co/wordpress/116016/malware/android-spyware-system-update.html]
[https://www.bleepingcomputer[.]com/news/security/new-android-malware-spies-on-you-while-posing-as-a-system-update/]

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:
  - **iOS** - version 14.4.2, 12.5.2 or later
  - **iPadOS** - version 14.4.2
  - **watchOS** - version 7.3.3 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.*