CERT-PH Cybersecurity Threat Feeds

Issue Date	February 18, 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:

- QNAP Patches Critical Vulnerability in Surveillance Station NAS App
- Apple Patches Severe MacOS Big Sur Data Loss Bug
- SHAREit Affected by Severe Flaws yet to be Fixed
- Avaddon Ransomware Decryptor Released, but Quickly Reacted

- CRITICAL
- URGENT
- INFORMATION

Description

QNAP Patches Critical Vulnerability in Surveillance Station NAS App

2021.02.17 | Source(s): Bleeping Computer

Analysis:

QNAP has addressed a critical security vulnerability in the Surveillance Station app that allows attackers to execute malicious code remotely on network-attached storage (NAS) devices running the vulnerable software. The critical security flaw patched by QNAP is a stack-based buffer overflow vulnerability impacting QNAP NAS devices running Surveillance Station. Successful exploitation of the vulnerability allows an attacker to to execute arbitrary code and regularly subvert any security service or anti-malware solutions running on the compromised device. Surveillance Station is QNAP's network surveillance Video Management System (VMS), a software solution that can help users manage and monitor up to 12 IP cameras. It is a Turbo NAS standard application with support for over 3,000 IP camera models, and it can be installed from the company's QTS App Center.

Read more:

[https://www.bleepingcomputer[.]com/news/security/qnap-patches-critical-vulnerability-in-surveillance-station-nas-app/]

Apple Patches Severe MacOS Big Sur Data Loss Bug

2021.02.16 | Source(s): ZDNet

Analysis:

Apple released a fix for a bug that could cause serious data loss and affects Apple's macOS Big Sur. The bug comes down to the macOS Big Sur installer not checking if the Mac has the required free space available to carry out an upgrade. The upgrade runs into problems, and if that isn't bad enough, if the user's Mac was encrypted using FileVault, then the user is locked out of their data.

Read more:

[https://www.zdnet[.]com/article/apple-patches-severe-macos-big-sur-data-loss-bug]

SHAREit Affected by Severe Flaws yet to be Fixed

2021.02.15 | Source(s): Security Affairs

Analysis:

SHAREit, a popular file-sharing Android app, was discovered to have multiple unpatched vulnerabilities. The vulnerabilities can lead to RCE on the devices where the app is installed. The vulnerabilities can be exploited to leak user's sensitive data, execute arbitrary code with SHAREit permissions, and lead to RCE. A second issue that experts discovered was the possibility for third parties to temporarily gain read/write access to FileProvider's data. Additionally, the app offers an option to install an APK with the file name suffix sapk, which an attacker could potentially abuse to install a malicious app.

Read more:

https://securityaffairs[.]co/wordpress/114636/mobile-2/shareit-app-flaw.html

Avaddon Ransomware Decryptor Released, but Quickly Reacted

2021.02.11 | Source(s): Security Affairs

Analysis:

Avaddon ransomware was decrypted with a free tool by security researchers, but its operators quickly revised the malware code to make it ineffective. The expert developed the AvaddonDecrypter utility used by victims of the ransomware when their computers should not have been powered off after the infection. This utility dumps the infected system's RAM memory and scans it for information that could help locate the encryption key. Upon receiving news of the decryption, Avaddon's operators updated their ransomware code to make it inefficient.

Read more:

https://securityaffairs[.]co/wordpress/114482/malware/avaddon-ransomware-decryptor.html

CERT-PH Recommendations:

o Update any vulnerable system/applications/devices to their latest and patched versions:

- MacOS Big Sur - version 11.2.1

- QNAP Surveillance Station

o 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.*