CERT-PH Cybersecurity Threat Feeds

Issue Date	May 04, 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:

- Pulse Secure Fixes Zero-day in Pulse Connect Secure (PCS) SSL VPN Actively Exploited
- N3TW0RM Ransomware Emerges in Wave of Cyberattacks
- Apple Fixes 2 iOS Zero-day Vulnerabilities Actively Used in Attacks
- Published PoC Exploit for Microsoft Exchange Flaw

- CRITICAL
- URGENT
- INFORMATION

Description

Pulse Secure Fixes Zero-day In Pulse Connect Secure (PCS) SSL VPN Actively Exploited

2021.05.03 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Pulse Secure addressed a zero-day vulnerability in the Pulse Connect Secure (PCS) SSL VPN appliance that is being actively exploited by threat actors in attacks against defense firms and government agencies. Tracked as CVE-2021-22893, the vulnerability is a buffer overflow issue in Pulse Connect Secure Collaboration Suite prior b9.1R11.4 that allows remote authenticated attackers to execute arbitrary code as the root user via a maliciously crafted meeting room. The attacks began in August 2020, when a group tracked as UNC2630, began targeting US defense contractors and European organizations. The vendor also released a tool that can scan Pulse Secure VPN servers for signs of compromise for CVE-2021-22893 or other previous vulnerabilities.

Read more:

[https://securityaffairs[.]co/wordpress/117484/hacking/pulse-connect-secure-zeroday.html]
[https://www.bleepingcomputer[.]com/news/security/pulse-secure-fixes-vpn-zero-day-used-to-hack-high-value-targets/]

N3TW0RM Ransomware Emerges in Wave of Cyberattacks

2021.05.03 | Source(s): Bleeping Computer

Analysis:

A new ransomware gang is targeting Israeli companies in a wave of cyberattacks. Dubbed as N3TW0RM, the gang created a data leak site where they threatened to leak stolen files as a way to scare their victims into paying a ransom. According to security experts, the N3TW0RM threat actors install a program on a victim's server that will listen for connections from the workstations. Threat actors then use PAExec to deploy and execute the 'slave.exe' client executable on every device that the ransomware will encrypt. When encrypting files, the files will have the '.n3tw0rm' extension appended to their names.

Read more:

[https://www.bleepingcomputer[.]com/news/security/n3tw0rm-ransomware-emerges-in-wave-of-cyberattacks-in-israel/]

Apple Fixes 2 iOS Zero-day Vulnerabilities Actively Used in Attacks

2021.05.03 | Source(s): Bleeping Computer, ZDNet

Analysis:

Apple released security updates that fix two actively exploited iOS zero-day vulnerabilities in the Webkit engine used by hackers to attack iPhones, iPads, iPods, macOS, and Apple Watch devices. Webkit is Apple's browser rendering engine that is required to be used by all mobile web browsers in iOS and other applications that render HTML, such as Apple Mail and the App Store. Tracked as CVE-2021-30665 and CVE-2021-30663, both vulnerabilities allow arbitrary remote code execution (RCE) on vulnerable devices simply by visiting a malicious website.

Read more:

[https://www.bleepingcomputer[.]com/news/apple/apple-fixes-2-ios-zero-day-vulnerabilities-actively-used-in-attacks/]
[https://www.zdnet.com/article/you-should-update-your-iphone-and-ipad-to-ios-14-5-1-right-away/]

Published PoC Exploit for Microsoft Exchange Flaw

2021.05.03 | Source(s): Security Affairs

Analysis:

Cybersecurity experts released technical details and proof-of-concept exploit (PoC) code for the high-severity vulnerability in Microsoft Exchange that could be exploited by remote attackers to execute arbitrary code on vulnerable systems. Tracked as CVE-2021-28482, the flaw is a remote code execution that could allow attacks to compromise vulnerable installs. The flaw received a CVSS base score of 8.8 out of 10 and for this reason, Microsoft urges its customers to install the latest updates.

Read more:

[https://securityaffairs[.]co/wordpress/117493/hacking/microsoft-exchange.html]

CERT-PH Recommendations:

- Pulse Connect Secure users are advised to run the Pulse Secure Integrity Tool first to determine if their devices were breached and to respond accordingly before installing the update.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **iOS** - version 14.5.1 and 12.5.3
  - **macOS Big Sur** - version 11.3.1
  - **watchOS** - version 7.4.1
  - Microsoft April 2021 Security Update
- 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.*