CERT-PH Cybersecurity Threat Feeds

Issue Date	April 22, 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:

- SonicWall Warns Customers to Patch 3 Zero-days Exploited in The Wild
- REvil Gang Tries to Extort Apple and Threatens to Sell Stolen Blueprints
- WhatsApp Pink Malware Can Now Auto-reply to User's Signal, Telegram and Viber Texts
- Google Fixes Exploited Chrome Zero-day Dropped on Twitter

- CRITICAL
- URGENT
- INFORMATION

Description

SonicWall Warns Customers to Patch 3 Zero-days Exploited in The Wild

2021.04.20 | Source(s): Bleeping Computer, Security Affairs

Analysis:

SonicWall is urging their customers to patch a set of three zero-day vulnerabilities affecting both its on-premises and hosted Email Security products. The three zero-days detected were an Email Security Pre-Authentication Administrative Account Creation vulnerability that allows an attacker to create an administrative account by sending a crafted HTTP request to the remote host, an Email Security Post-Authentication Arbitrary File Creation vulnerability that allows a post-authenticated attacker to upload an arbitrary file to the remote host, an Email Security Post-Authentication Arbitrary File Read vulnerability that enables a post-authenticated attacker to read an arbitrary file from the remote host and were tracked as CVE-2021-20021, CVE-2021-20022 and CVE-2021-20023, respectively. According to security researchers, threat actors leverage these flaws to install a backdoor, access files and emails, and move laterally into the victim organization's network.

Read more:

[https://www.bleepingcomputer[.]com/news/security/sonicwall-warns-customers-to-patch-3-zero-days-exploited-in-the-wild/]
[https://securityaffairs[.]co/wordpress/117075/hacking/sonicwall-es-zerodays.html]

REvil Gang Tries to Extort Apple and Threatens to Sell Stolen Blueprints

2021.04.20 | Source(s): Bleeping Computer, The Hacker News

Analysis:

The REvil ransomware gang wants Apple to pay stolen product blueprints to avoid having them leaked on REvil's leak site. REvil tried to extort Apple only after Quanta Computer, a leading notebook manufacturer and one of Apple's business partners, refused to communicate with the ransomware gang or pay the ransom demanded after they allegedly stole "a lot of confidential data" from Quanta's network. According to security experts, based on the negotiation chat on REvil's payment site, REvil warned that "drawings of all Apple devices and all personal data of employees and customers will be published with subsequent sale" if Quanta did not begin negotiating a ransom. REvil leaked over a dozen schematics and diagrams of MacBook components on its dark web leak site, although there is no indication that any of them are new Apple products.

Read more:

[https://www.bleepingcomputer.com/news/security/revil-gang-tries-to-extort-apple-threatens-to-sell-stolen-blueprints/]
[https://thehackernews[.]com/2021/04/hackers-threaten-to-leak-stolen-apple.html]

WhatsApp Pink Malware Can Now Auto-reply to User's Signal, Telegram and Viber Texts

2021.04.21 | Source(s): Bleeping Computer, Security Affairs

Analysis:

A WhatsApp malware has been updated with advanced capabilities that let this counterfeit Android app automatically respond to user's Signal, Telegram, Viber, and Skype messages. Dubbed as WhatsApp Pink, the malware is a counterfeit of the popular messaging app WhatsApp that targets WhatApp users, contains a trojan that takes over the victim's Android device and spreads itself to other users. According to security researchers, the malware is being advertised as a new WhatsApp app in pink in group messages. Once the ad is clicked, it will then download the malicious WhatsApp Pink APK. The malware is capable of auto-responding to messages in various apps such as Signal, Viber, Telegram and Skype. Although end-to-end encrypted messaging apps protect communications and messages in transit, like any end-to-end encrypted system, the data at rest can itself be accessible to the person holding the device, or applications, such as malware, running on the device.

Read more:

[https://www.bleepingcomputer[.]com/news/security/whatsapp-pink-malware-can-now-auto-reply-to-your-signal-telegram-texts/]
[https://securityaffairs[.]co/wordpress/117094/malware/whatsapp-pink-malware.html]

Google Fixes Exploited Chrome Zero-day Dropped on Twitter

2021.04.21 | Source(s): Bleeping Computer

Analysis:

Google released Chrome 90.0.4430.85 to address an actively exploited zero-day and four other high severity security vulnerabilities impacting today's most popular web browser. Tracked as CVE-2021-21224, the zero-day vulnerability was described as a type confusion in V8. This remote code execution vulnerability cannot be exploited by attackers to escape Chromium's sandbox security feature. However, it can be chained with another security bug that can allow the exploit to escape the sandbox and execute arbitrary code on the targeted users' systems. In addition, Google also fixed four other high severity vulnerabilities in Chrome, a heap buffer overflow in V8, an integer overflow in Mojo, an out of bounds memory access in V8 and a use after free in navigation tracked as CVE-2021-21222, CVE-2021-21223, CVE-2021-21225 and CVE-2021-21226 respectively.

Read more:

[https://www.bleepingcomputer[.]com/news/security/google-fixes-exploited-chrome-zero-day-dropped-on-twitter-last-week/]

CERT-PH Recommendations:

- Users are advised to avoid installing unknown or unverified applications, especially from third-party distribution platforms. Scrutinize the application's permissions before installation and avoid allowing apps to view unnecessary information and other application's data.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Email Security (Windows)** - version 10.0.9.6173
  - **Email Security (Hardware & ESXi Virtual Appliance)** - version 10.0.9.6177
  - **Hosted Email Security** - version 10.0.9.6173
  - **Google Chrome** - version 90.0.4430.85
- Android users are urged to check their devices and immediately uninstall and remove the following applications:
  - **WhatsApp Pink**
- 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.*