CERT-PH Cybersecurity Threat Feeds

Issue Date	February 05, 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:

- Hacking Group Also Used an IE Zero-day Against Security Researchers
- SonicWall Released Patch for Actively Exploited SMA 100 Zero-Day
- Google Addresses Chrome Zero-day Flaw Actively Exploited in The Wild
- Critical Bugs in Realtek Wi-Fi Module for Embedded Devices

- CRITICAL
- URGENT
- INFORMATION

Description

Hacking Group Also Used an IE Zero-day Against Security Researchers

2021.02.04 | Source(s): Bleeping Computer

Analysis:

Researchers discovered an Internet Explorer zero-day vulnerability used in recent North Korean attacks against security and vulnerability researchers. Tracked as Lazarus, the North Korean state-sponsored hacking group targets security researchers with MIME HTML (MHTML) files in this social engineering campaign. After analysis it was discovered that the payloads downloaded by the MHT file contains an exploit for an Internet Explorer zero-day vulnerability that when exploited, may allow the attackers to upload a list of the running process, screen captures, and network information to their command and control server. It would then download and execute additional malicious code from the C2 server to be executed.

Read more:

[https://www.bleepingcomputer[.]com/news/security/hacking-group-also-used-an-ie-zero-day-against-security-researchers/]

SonicWall Released Patch for Actively Exploited SMA 100 Zero-Day

2021.02.04 | Source(s): Security Affairs

Analysis:

SonicWall has released a security patch to address the zero-day flaw actively exploited in attacks against the Secure Mobile Access (SMA) 100 series appliances. Tracked as CVE-2021-20016, is a vulnerability rated as critical with a CVSS score of 9.8 and exists due to improper SQL command neutralization in the SonicWall SSLVPN SMA100 product, it could be exploited by a remote, unauthenticated attacker for credential access on SMA100 build version 10.x.

Read more:

[https://securityaffairs[.]co/wordpress/114197/hacking/sonicwall-zero-day-patch.html]

Google Addresses Chrome Zero-day Flaw Actively Exploited in The Wild

2021.02.04 | Source(s): Security Affairs

Analysis:

Google released Chrome 88.0.4324.150 version that addressed an actively exploited zero-day security vulnerability. Tracked as CVE-2021-21148, is a vulnerability Heap buffer overflow that resides in the V8, which is an open-source high-performance JavaScript and WebAssembly engine, written in C++ and is rated by Google as high severity.

Read more:

[https://securityaffairs[.]co/wordpress/114224/hacking/google-chrome-zero-day.html]

Critical Bugs in Realtek Wi-Fi Module for Embedded Devices

2021.02.04 | Source(s): Hacker News

Analysis:

Google removed the popular The Great Suspender from the official Chrome Web Store for containing Major vulnerabilities have been discovered in the Realtek RTL8195A Wi-Fi module that could have been exploited to gain root access and take complete control of a device's wireless communications. The flaws concern a mix of stack overflow, and out-of-bounds reads that stem from the Wi-Fi module's WPA2 four-way handshake mechanism during authentication. Among the flaws, tracked as CVE-2020-9395, is a buffer overflow vulnerability that permits an attacker in the proximity of an RTL8195 module to completely take over the module, without having to know the Wi-Fi network password and regardless of whether the module is acting as a Wi=Fi access point or client. The Realtek RTL8195A module is a standalone, low-power-consumption Wi-Fi hardware module targeted at embedded devices used in several industries such as agriculture, smart home, healthcare, gaming, and automotive sectors.

Read more:

[https://thehackernews[.]com/2021/02/critical-bugs-found-in-popular-realtek.html]

CERT-PH Recommendations:

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

- **SonicWall Firmware** - version 10.2.0.5-29sv
- **SMA 200, SMA 210, SMA 400, SMA 410**
- **SMA 500v (Azure, AWS, ESXi, HyperV)**
- **Google Chrome** - version 88.0.4324.150
- **Realtek** - Ameba Arduino 2.0.8

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.*