CERT-PH Cybersecurity Threat Feeds

Issue Date	May 03, 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:

- **New Ransomware Group Uses SonicWall Flaw To Breach Networks**
- **Command Injection Flaw In PHP Composer Allowed Supply-Chain Attacks**
- **Microsoft Warns of 25 Critical Vulnerabilities in IoT, Industrial Devices**
- **APT Group Uses A New Backdoor in Attacks At Russian Defense Contractor**

- CRITICAL
- URGENT
- INFORMATION

Description

New Ransomware Group Uses SonicWall Flaw To Breach Networks

2021.04.29 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Threat actors are discovered to be exploiting a zero-day bug in SonicWall SMA 100 Series VPN appliances to deploy new ransomware. Dubbed as FiveHands, the ransomware was being utilized by the threat group known as UNC2447, that targets vulnerable SonicWall internal systems. Tracked as CVE-2021-20016, an improper SQL command neutralization in the SonicWall SSLVPN SMA100 product that allows remote exploitation for credential access by an unauthenticated attacker. The ransomware exhibits similar functionalities as that of the HelloKitty ransomware. According to security experts, FiveHands added extra functionality to the ransomware, where it can also use the Windows Restart Manager to close a file currently in use so that it can be unlocked and successfully encrypted. It further differs by using different embedded encryption libraries, a memory-only dropper, and asynchronous I/O requests, not present in the HelloKitty ransomware strains in its family.

Read more:

[https://www.bleepingcomputer[.]com/news/security/new-ransomware-group-uses-sonicwall-zero-day-to-breach-networks/]
[https://securityaffairs[.]co/wordpress/117387/malware/unc2447-sonicwall-zero-day.html]

Command Injection Flaw In PHP Composer Allowed Supply-Chain Attacks

2021.04.29 | Source(s): Security Affairs, The Hacker News

Analysis:

The maintainers of the PHP Composer package have addressed a critical vulnerability that could have allowed an attacker to execute arbitrary commands and establish a backdoor in every PHP package. Tracked as CVE-2021-29472, the flaw is a command injection security vulnerability that stems from improper sanitization of URLs for repositories in root composer.json files and package source download URLs that could be interpreted as options for system commands executed by Composer. Composer is the major tool to manage and install software dependencies, it uses the online service Packagist to determine the correct supply chain for package downloads. Successful exploitation of the flaw could be used to further conduct supply-chain attack to organizations.

Read more:

[https://securityaffairs[.]co/wordpress/117366/security/php-composer-flaw.html]
[https://thehackernews[.]com/2021/04/a-new-php-composer-bug-could-enable.html]

Microsoft Warns of 25 Critical Vulnerabilities in IoT, Industrial Devices

2021.04.29 | Source(s): Bleeping Computer, Threatpost, Security Affairs

Analysis:

Cybersecurity experts discovered over two dozen critical remote code execution (RCE) vulnerabilities in Internet of Things (IoT) devices and Operational Technology (OT) industrial systems. Collectively known as BadAlloc, the flaws are caused by memory allocation Integer Overflow or Wraparound bugs. The vulnerabilities were found in standard memory allocation functions widely used in multiple real-time operating systems (RTOS), C standard library (libc) implementations, and embedded software development kits (SDKs). Threat actors could exploit the memory allocation function to perform a heap overflow, resulting in execution of malicious code on a vulnerable IOT and OT devices.

Read more:

[https://www.bleepingcomputer[.]com/news/security/microsoft-finds-critical-code-execution-bugs-in-iot-ot-devices/]
[https://threatpost[.]com/microsoft-warns-25-critical-iot-industrial-devices/165752/]
[https://securityaffairs[.]co/wordpress/117372/iot/badalloc-vulnerabilities-ot-iot.html]

APT Group Uses A New Backdoor in Attacks At Russian Defense Contractor

2021.04.28 | Source(s): The Hacker News

Analysis:

China-linked threat actors used a new malware to infiltrate the systems of an engineering company that designs submarines for the Russian Navy. Dubbed as PortDoor, the backdoor implements multiple functionalities, including the ability to do reconnaissance, target profiling, delivery of additional payloads, privilege escalation, process manipulation static detection antivirus evasion, one-byte XOR encryption, AES-encrypted data exfiltration. According to the security experts, the method of delivering the backdoor was a weaponized Rich Text File (RTF) document attached to an email. The weaponized RTF documents generated with the exploit builder are able to trigger the CVE-2017-11882, CVE-2018-0798, CVE-2018-0802 vulnerabilities in Microsoft's Equation Editor.

Read more:

[https://www.bleepingcomputer[.]com/news/security/suspected-chinese-state-hackers-target-russian-submarine-designer/]
[https://securityaffairs[.]co/wordpress/117396/apt/china-linked-apt-russia-contractor.html]

CERT-PH Recommendations:

- Affected IOT and OT devices by BadAlloc are as follows:
    - Amazon FreeRTOS, Version 10.4.1
    - Apache Nuttx OS, Version 9.1.0
    - ARM CMSIS-RTOS2, versions prior to 2.1.3
    - ARM Mbed OS, Version 6.3.0
    - ARM mbed-uallaoc, Version 1.3.0
    - Cesanta Software Mongoose OS, v2.17.0
    - eCosCentric eCosPro RTOS, Versions 2.0.1 through 4.5.3
    - Google Cloud IoT Device SDK, Version 1.0.2
    - Linux Zephyr RTOS, versions prior to 2.4.0
    - MediaTek LinkIt SDK, versions prior to 4.6.1
    - Micrium OS, Versions 5.10.1 and prior
    - Micrium uCOS II/uCOS III Versions 1.39.0 and prior
    - NXP MCUXpresso SDK, versions prior to 2.8.2
    - NXP MQX, Versions 5.1 and prior
    - Redhat newlib, versions prior to 4.0.0
    - RIOT OS, Version 2020.01.1
    - Samsung Tizen RT RTOS, versions prior 3.0.GBB
    - TencentOS-tiny, Version 3.1.0
    - Texas Instruments CC32XX, versions prior to 4.40.00.07
    - Texas Instruments SimpleLink MSP432E4XX
    - Texas Instruments SimpleLink-CC13XX, versions prior to 4.40.00
    - Texas Instruments SimpleLink-CC26XX, versions prior to 4.40.00
    - Texas Instruments SimpleLink-CC32XX, versions prior to 4.10.03
    - Uclibc-NG, versions prior to 1.0.36
    - Windriver VxWorks, prior to 7.0
- Users of the above software and applications are advised to:
    - Regular network security monitoring to detect any suspicious and/or unknown network behavior.

    - Strengthening network segmentation and isolate critical assets from the business network.
    - Minimize network exposure for all control system devices and/or systems and ensure that they are not accessible from the Internet.
    - Regular patching and security updates
- Update any vulnerable system/applications/devices to their latest and patched versions:
    - **SonicWall SSLVPN SMA100** - version 10.2.0.5-d-29sv or later
    - **PHP Composer** - version 2.0.13 or 1.10.22
- 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.*