CERT-PH Cybersecurity Threat Feeds

Issue Date	March 16, 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:

- DearCry Ransomware Attacks Microsoft Exchange With ProxyLogon Exploits
- 15-year-old Linux Kernel Bugs Let Attackers Gain Root Privileges
- Google Fixes The Third Actively Exploited Chrome Zero-Day
- 15 Flaws Found in Netgear JGS516PE Switch, Including A Critical RCE

- CRITICAL
- URGENT
- INFORMATION

Description

DearCry Ransomware Attacks Microsoft Exchange With ProxyLogon Exploits

2021.03.11 | Source(s): Bleeping Computer

Analysis:

Threat actors are now installing a new ransomware after hacking into Microsoft Exchange servers using the recently disclosed ProxyLogon vulnerabilities. Dubbed as DearCry, the ransomware will create a Windows service named 'msupdate' that is started to perform the encryption. This Windows service is later removed when the encryption process is finished. When encrypting files, it will append the .CRYPT extension to the file's name and prepend the 'DEARCRY!' string to the beginning of each encrypted file. According to cybersecurity experts, the ransomware uses AES-256 to encrypt the files and the RSA-2048 public key to encrypt the AES key.

Read more:

[https://www.bleepingcomputer[.]com/news/security/dearcry-ransomware-attacks-microsoft-exchange-with-proxylogon-exploits/]

15-year-old Linux Kernel Bugs Let Attackers Gain Root Privileges

2021.03.11 | Source(s): Security Affairs

Analysis:

Cybersecurity experts discovered three 15-year-old flaws in Linux kernel that could be exploited by local attackers with basic user privileges to gain root privileges on vulnerable Linux systems. The flaws exist in the SCSI (Small Computer System Interface) which defines both a parallel I/O bus and a data protocol to connect a wide variety of peripherals to host a computer. The three vulnerabilities were a heap buffer overflow, a kernel pointer leak and an out-of-bounds tracked as CVE-2021-27365, CVE-2021-27363 and CVE-2021-27364 respectively. Successful exploitation of these vulnerabilities may allow attackers to bypass the security features Kernel Address Space Layout Randomization (KASLR) bypass, Supervisor Mode Execution Protection (SMEP), Supervisor Mode Access Prevention (SMAP), and Kernel Page-Table Isolation (KPTI). These flaws can also lead to data leaks and trigger denial of service conditions.

Read more:

[https://securityaffairs[.]co/wordpress/115565/security/linux-kernel-flaws.html]
[https://www.bleepingcomputer[.]com/news/security/15-year-old-linux-kernel-bugs-let-attackers-gain-root-privileges/]

Google Fixes The Third Actively Exploited Chrome Zero-Day

2021.03.15 | Source(s): Security Affairs, Threatpost, Bleeping Computer

Analysis:

Google has addressed a new zero-day flaw in its Chrome browser that has been actively exploited in the wild, the second one within a month. Tracked as CVE-2021-21193, the flaw is a use after free vulnerability in the Blink rendering engine which relates to incorrect use of dynamic memory during program operation. The flaw received a CVSS score of 8.8 out of 10. Successful exploitation may allow remote code-execution and denial-of-service attacks on affected systems.

Read more:
[https://www.bleepingcomputer[.]com/news/security/google-fixes-second-actively-exploited-chrome-zero-day-this-month/]
[https://securityaffairs[.]co/wordpress/115600/security/google-chrome-0-day.html]
[https://threatpost[.]com/google-mac-windows-chrome-zero-day/164759/]

15 Flaws Found in Netgear JGS516PE Switch, Including A Critical RCE

2021.03.14 | Source(s): Security Affairs

Analysis:

Netgear has released security and firmware updates for its JGS516PE Ethernet switch to address 15 vulnerabilities, including a critical remote code execution issue. Tracked as CVE-2020-26919, the critical flaw resides in the switch internal management web application in firmware versions prior to 2.6.0.43, it could be exploited by unauthenticated attackers to bypass authentication and execute actions with administrator privileges. The vulnerability received a CVSS score of 9.8 out of 10.

Read more:
[https://securityaffairs[.]co/wordpress/115586/hacking/netgear-soho-flaws.html]

CERT-PH Recommendations:

- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Microsoft Exchange Server**- March Security Update
  - **Linux Systems** - latest version
  - **Google Chrome** - version 89.0.4389.90 or later
  - **Netgear JGS516PE** - version 2.6.0.48. or later
- 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.*