CERT-PH Cybersecurity Threat Feeds

Issue Date	May 05, 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:

- Vulnerable Dell Driver Puts Hundreds of Millions of Systems at Risk
- Worldwide Phishing Attacks Deliver Three New Malware Strains
- Project Signal, A State-Sponsored Ransomware Operation
- Critical 21Nails Exim Bugs Expose Millions of Servers to Attacks

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

Vulnerable Dell Driver Puts Hundreds of Millions of Systems At Risk

2021.05.04 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Cybersecurity experts discovered a driver that's been pushed for the past 12 years to Dell computer devices for consumers and enterprises contains multiple vulnerabilities that could lead to increased privileges on affected system. Collectively tracked as CVE-2021-21551, the five flaws reside in DBUtil, a driver from Dell machines that install and load during the BIOS update process and is unloaded at the next reboot. Successful exploitation of the vulnerability may allow escalation of privileges from a non-administrator user to kernel mode privileges. In addition, it allows threat actors and malware to gain persistence on the infected system. According to security experts, although there is a single tracking number, there are five separate flaws, most of them leading to privilege escalation and one code logic issue that leads to denial of service. Affected users includes users who updated the vulnerable dbutil_2_3.sys driver via affected firmware update utility packages, or via Dell Command Update, Dell Update, Alienware Update, Dell System Inventory Agent, or Dell Platform Tags, including when using any Dell notification solution to update drivers, BIOS, or firmware on your system

Read more:

[https://www.bleepingcomputer[.]com/news/security/vulnerable-dell-driver-puts-hundreds-of-millions-of-systems-at-risk/]
[https://securityaffairs[.]co/wordpress/117514/security/cve-2021-21551-dell-flaws.html]

Worldwide Phishing Attacks Deliver Three New Malware Strains

2021.05.04 | Source(s): Bleeping Computer, Threatpost

Analysis:

A global-scale phishing campaign targeted worldwide organizations across an extensive array of industries with never-before-seen malware strains delivered via specially-tailored lures. Cybersecurity experts linked this campaign with the threat group dubbed as UNC2529. Within the campaign, threat actors deployed three new malware strains onto the targets' computers using custom phishing lures. According to security experts, throughout the two waves of attacks, the threat group used phishing emails with links to a JavaScript-based downloader, dubbed DOUBLEDRAG, or an Excel document with an embedded macro that downloaded an in-memory PowerShell-based dropper, known as DOUBLEDROP, from attackers' command-and-control (C2) servers. The DOUBLEDROP dropper bundles 32 and 64-bit instances of a backdoor, named DOUBLEBACK, implemented as a PE dynamic library. The backdoor gets injected into the PowerShell process spawned by the dropper and is still designed to later attempt to inject itself into a newly spawned Windows Installer (msiexec.exe) process if Bitdefender's antivirus engine is not running on the compromised computer. In the final stage, the DOUBLEBACK backdoor loads its plugin and reaches out to the C2 server in a loop to fetch commands to execute on the infected device.

Read more:

[https://www.bleepingcomputer[.]com/news/security/worldwide-phishing-attacks-deliver-three-new-malware-strains/]
[https://threatpost[.]com/global-phishing-attacks-new-malware-strains/165857/]

Project Signal, A State-Sponsored Ransomware Operation

2021.05.05 | Source(s): Security Affairs

Analysis:

Researchers have uncovered a state-sponsored ransomware campaign conducted by Iran's Islamic Revolutionary Guard Corps (IRGC) through an Iranian contracting company called Emen Net Pasargard (ENP) (aka "Imannet Pasargad," "Iliant Gostar Iranian," "Eeleyanet Gostar Iraniyan"). ENP is controlled by Iran's intelligence services and supports Iran's Islamic Revolutionary Guard Corps (IRGC), the IRGC Quds Force (IRGC-QF), and Iran's Ministry of Intelligence and Security (MOIS). Tracked as Project Signal, the ransomware campaign started between late July 2020 and early September 2020 and was conducted with financial motivations. According to security experts, as is true for ENP's Project Signal, if Pay2Key is sponsored by Iran, it's possible the appearance of financial motivation could have been an obfuscation technique designed to mimic a cybercriminal group. At this point in time, cybersecurity experts can neither confirm any attributes of Project Signal targets nor if there is any link between ENP's Project Signal and Pay2Key.

Read more:

[https://securityaffairs[.]co/wordpress/117506/apt/iran-state-sponsored-ransomware.html]

Critical 21Nails Exim Bugs Expose Millions of Servers to Attacks

2021.05.04 | Source(s): Bleeping Computer

Analysis:

Cybersecurity researchers discovered critical vulnerabilities in the Exim mail transfer agent (MTA) software allowing unauthenticated remote attackers to execute arbitrary code and gain root privilege on mail servers with default or common configurations. Collectively tracked as 21Nails, the security flaws consist of 10 remotely exploitable and 11 locally exploitable flaws affecting Exim versions released before 4.94.2. Some of the vulnerabilities can be chained together to obtain a full remote unauthenticated code execution and gain root privileges on the Exim Server. Exim is the default MTA on Debian Linux distros and currently the world's most popular MTA, according to a mail server survey from May 1st, 2021. Successful exploitation of the vulnerabilities could allow threat actors to modify sensitive email settings on the mail servers and allow adversaries to create new accounts on the target mail servers.

Read more:

[https://www.bleepingcomputer[.]com/news/security/critical-21nails-exim-bugs-expose-millions-of-servers-to-attacks/]

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.
- Impacted Dell users are advised to immediately remove the vulnerable dbutil_2_3.sys driver from the affected system.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Dell System Inventory Agent** - version 2.6.0.0 or later
  - **Exim** - version 4.94.2 or later
  - **Dell Command Update, Dell Update, or Alienware 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.*