CERT-PH Cybersecurity Threat Feeds

Issue Date	January 11, 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:

- NVIDIA Fixes High Severity Flaws Affecting Windows, Linux Devices
- Bugs in Firefox, Chrome, Edge Allow Remote System Hijacking
- TeamTNT Botnet Now Steals Docker API And AWS Credentials
- WhatsApp Will Share Your Data With Facebook And Its Companies

- CRITICAL
- URGENT
- INFORMATION

Description

NVIDIA Fixes High Severity Flaws Affecting Windows, Linux Devices

2021.01.08 | Source(s): Bleeping Computer, ZDNet

Analysis:

NVIDIA has released security updates to address six security vulnerabilities found in Windows and Linux GPU display drivers, as well as ten additional flaws affecting the NVIDIA Virtual GPU (vGPU) management software. The vulnerabilities expose Windows and Linux machines to attacks leading to denial of service (DoS), escalation of privileges, data tampering, or information disclosure. The bugs come with CVSS V3 base scores ranging from 5.3 to 8.4, with 11 of them having received a high-risk assessment from NVIDIA.

Read more:

[https://www.bleepingcomputer[.]com/news/security/nvidia-fixes-high-severity-flaws-affecting-windows-linux-devices/]

[https://www.zdnet[.]com/article/nvidia-releases-security-update-for-high-severity-graphics-driver-vulnerabilities/]

Bugs in Firefox, Chrome, Edge Allow Remote System Hijacking

2021.01.08 | Source(s): Threatpost

Analysis:

Makers of the Chrome, Firefox and Edge browsers are urging users to patch critical vulnerabilities that if exploited allow hackers to hijack systems running the software. Tracked as CVE-2020-16044, is a vulnerability classified as a use-after-free bug and tied to the way Firefox handles browser cookies and if exploited allows hackers to gain access to the computer, phone or tablet running the browser software. For Google's Chrome browser, an out-of-bounds write bug, tracked as CVE-2020-15995, in V8 exists and is classified as high severity. Researchers believed that similar to out of bounds write in V8 bugs, the flaw could allow remote attackers to exploit a heap corruption via a crafted HTML page.

Read more:

[https://threatpost[.]com/firefox-chrome-edge-bugs-system-hijacking/162873/]

TeamTNT Botnet Now Steals Docker API And AWS Credentials

2021.01.10 | Source(s): Security Affairs

Analysis:

Cybersecurity experts discovered that the TeamTNT botnet was improved and is now able to steal Docker credentials. The TeamTNT botnet is a crypto-mining malware operation that targets Docker installs. Upon infection, the bot scans for ~/.aws/credentials and ~/.aws/config that are the paths where the AWS CLI stores credentials and configuration details in an unencrypted file. The malware deploys the XMRig mining tool to mine Monero cryptocurrency. The new variant of the bot is also able to collect Docker API credentials using a routine that only checks for credential files on the machine and then exfiltrates them.

Read more:

[https://securityaffairs[.]co/wordpress/113228/malware/teamtnt-botnet-docker-aws.html]

WhatsApp Will Share Your Data with Facebook And Its Companies

2021.01.06 | Source(s): Security Affairs, Bleeping Computer

Analysis:

WhatsApp is notifying its users through the mobile app that, starting February, they will be required to share their data with Facebook and its companies such as Facebook, Facebook Payments, Onavo, Facebook Technologies, and CrowdTangle. If the user refuses to accept the new policy, will not be able to access their accounts and could delete their account altogether. The move aims at improving the users' experience with targeting advertising. WhatsApp currently shares specific information with Facebook companies, including account registration data, transaction data, and service-related information.

Read more:

[https://www.bleepingcomputer[.]com/news/security/windows-psexec-zero-day-vulnerability-gets-a-free-micropatch/]

CERT-PH Recommendations:

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

- GeForce, NVIDIA RTX, Quadro, NVS, Tesla GPU display drivers, Virtual GPU Manager and guest driver software

- NVIDIA - January Security Update

- Firefox - Desktop 84.0.2,

- Android - version 84.1.3

- Corporate ESR Firefox - version 78.6.1

- Microsoft Edge browser - version 87.0.664.75

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.