CERT-PH Cybersecurity Threat Feeds

Issue Date	March 03, 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:

- Malicious NPM Packages Target Amazon, Slack With New Dependency Attacks
- Google Fixes Second Actively Exploited Chrome Zero-day Bug This Year
- Alleged China-linked APT41 Group Targets Indian Critical Infrastructures
- Microsoft Fixes Actively Exploited Exchange Zero-day Bugs

- CRITICAL
- URGENT
- INFORMATION

Description

Beware: AOL Phishing Email States your Account will be Closed

2021.02.28 | Source(s): Bleeping Computer

Analysis:

Threat actors are targeting Amazon, Zillow, Lyft, and Slack NodeJS apps using a new 'Dependency Confusion' vulnerability to steal Linux/Unix password files and open reverse shells back to the attackers. This flaw works by attackers creating packages utilizing the same names as a company's internal repositories or components. When hosted on public repositories, including npm, PyPI, and RubyGems, dependency managers would use the packages on the public repo rather than the company's internal packages when building the application This "dependency confusion" would allow an attacker to inject their own malicious code into an internal application in a supply-chain attack.This "dependency confusion" would allow an attacker to inject their own malicious code into an internal application in a supply-chain attack. The malicious packages are named 'amzn', 'zg-rentals', 'lyft-dataset-sdk', 'serverless-slack-app' and utilize similar names as known repositories on GitHub and other projects

Read more:

[https://www.bleepingcomputer[.]com/news/security/malicious-npm-packages-target-amazon-slack-with-new-dependency-attacks/]

Google Fixes Second Actively Exploited Chrome Zero-day Bug This Year

2021.03.02 | Source(s): Bleeping Computer

Analysis:

Google has fixed an actively exploited zero-day vulnerability in the Chrome 89.0.4389.72 version to the Stable desktop channel for Windows, Mac, and Linux users. Tracked as CVE-2021-2114, the flaw is a heap buffer overflow bug in V8 and rated as high severity.

Read more:

[https://www.bleepingcomputer[.]com/news/security/google-fixes-second-actively-exploited-chrome-zero-day-bug-this-year/]

Alleged China-linked APT41 Group Targets Indian Critical Infrastructures

2021.03.02 | Source(s): Security Affairs

Analysis:

Security researchers spotted a suspected Chinese APT actor targeting critical infrastructure operators in India. The list of targets includes power plants, electricity distribution centers, and seaports in the country. Tracked as RedEcho, the APT group also targeted a high-voltage transmission substation and a coal-fired thermal power plant. Researchers identified 21 IP addresses associated with 10 distinct Indian organizations in the power generation and the transmission sector that were targeted as part of this campaign. Experts determined that two additional critical infrastructures targeted by the group were in the maritime industry.

Read more:

[https://securityaffairs[.]co/wordpress/115156/apt/china-apt41-india.html]

Microsoft Fixes Actively Exploited Exchange Zero-day Bugs

2021.02.27 | Source(s): Security Affairs

Analysis:

Microsoft has released emergency out-of-band security updates for all supported Microsoft Exchange versions that fix four zero-day vulnerabilities actively exploited in targeted attacks. The flaws were a server-side request forgery (SSRF) vulnerability in Exchange, an insecure deserialization vulnerability in the Unified Messaging service, and two post-authentication arbitrary file write vulnerabilities in Exchange. These four zero-day vulnerabilities are tracked as CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065 respectively and are chained together to gain access to Microsoft Exchange servers, steal email, and plant further malware for increased access to the network.

Read more:

[https://www.bleepingcomputer[.]com/news/security/microsoft-fixes-actively-exploited-exchange-zero-day-bugs-patch-now/]

CERT-PH Recommendations:

- Users are advised to be cautious and always check the authenticity of the website before giving any private information or login credentials. Phishing attacks often use multiple redirects and unsecure connections before landing on the attacker's controlled website. If unsure of the website visited and causes to raise red flags, immediately put the website in your browser's list of locked webpages.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Google Chrome** - version 89.0.4389.72
  - **Microsoft Exchange** - March 2021 Security Updates
- 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.*