CERT-PH Cybersecurity Threat Feeds

Issue Date	January 28, 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:

- New Linux SUDO Flaw Lets Local Users Gain Root Privileges
- Apple Addresses Three iOs Zero-day Flaws Exploited in The Wild
- LogoKit, a New Phishing Kit That Dynamically Creates Phishing Forms
- Lebanese Cedar APT Group Broke into Telco and ISPs Worldwide

- CRITICAL
- URGENT
- INFORMATION

Description

New Linux SUDO Flaw Lets Local Users Gain Root Privileges

2021.01.27 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Security researchers discovered and fixed a Sudo vulnerability that allowed any local user to gain root privileges on Unix-like operating systems without requiring authentication. Tracked as CVE-2021-3156, is a Sudo privilege escalation vulnerability, a heap-based buffer overflow exploitable by any local user, with attackers not being required to know the user's password to successfully exploit the flaw. Sudo is a Unix program that enables system admins to provide limited root privileges to normal users listed in the sudoers file, while at the same time keeping a log of their activity.

Read more:

[https://www.bleepingcomputer[.]com/news/security/new-linux-sudo-flaw-lets-local-users-gain-root-privileges/]
[https://securityaffairs[.]co/wordpress/113900/hacking/sudo-vulnerability-cve-2021-3156.html]

Apple Addresses Three iOs Zero-day Flaws Exploited in The Wild

2021.01.27 | Source(s): Security Affairs, Threatpost

Analysis:

Apple has addressed three zero-day vulnerabilities in iOS that have been exploited in the wild with the release of security updates iOS 14.4. The flaws fixed were a race condition that resides in the iOS operating system kernel and the other two flaws resides in the WebKit browser engine. Tracked as CVE-2021-1782, CVE-2021-1870 and CVE-2021-1871, respectively. Successful exploitation may allow a remote attacker to cause arbitrary code execution.

Read more:

[https://securityaffairs[.]co/wordpress/113914/hacking/apple-ios-zero-day.html]
[https://threatpost[.]com/apple-patches-zero-days-ios-emergency-update/163374/]

LogoKit, a New Phishing Kit That Dynamically Creates Phishing Forms

2021.01.28 | Source(s): Security Affairs, Threatpost

Analysis:

Researchers discovered a new phishing kit that dynamically composes phishing content. Dubbed as LogoKit, is an embeddable set of JavaScript functions. The kit uses specially crafted URLs containing the email address of the recipient. The crafted URLs contain the email as a location hash. Upon navigating the URL, the LogoKit kit fetches the company logo from a third-party service and auto-fills the landing page with the victim's username or email address in order to trick victims into feeling like they have previously logged into the site. Once the victim entered its password, LogoKit performs an AJAX request, sending the recipient's credentials to an external source, and, finally, redirecting it to their corporate web site.

Read more:

[https://securityaffairs[.]co/wordpress/113961/cyber-crime/logokit-phishing-kit.html]
[https://threatpost[.]com/logokit-simplifies-office-365-sharepoint-login-phishing-pages/163430/]

Lebanese Cedar APT Group Broke into Telco and ISPs Worldwide

2021.01.28 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Researchers linked the Lebanese Cedar group known as Volatile Cedar, to a cyber espionage campaign that targeted companies around the world.The attacks began in early 2020 and threat actors breached internet service providers worldwide including in US, UK and UAE. Threat actors focus on intelligence gathering and the theft of sensitive data from targeted companies. The Lebanese Cedar hackers used open-source hacking tools to scan the internet for unpatched Atlassian and Oracle servers, then they used exploits to gain access to the server and deploy a web shell to gain a foothold in the target system. Once inside the target networks, the attackers deployed the Explosive remote access trojan (RAT), a malware exclusively used by the Lebanese Cedar group in past attacks.

Read more:

[https://securityaffairs[.]co/wordpress/113975/apt/lebanese-cedar-apt-attacks.html]
[https://www.bleepingcomputer[.]com/news/security/hezbollah-hackers-attack-unpatched-atlassian-servers-at-telcos-isps/]

CERT-PH Recommendations:

o System admins who use Sudo to delegate root privileges to their users should immediately upgrade to sudo 1.9.5p2 or later as soon as possible.

o 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

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

- **Sudo** - version 1.9.5p2 or later
- **iOS** - version 14.4

o Users of NetExtender VPN client and Secure Mobile Access are advised to check the advisory published by Sonicwall and apply necessary mitigation measures while waiting for the security patch

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.

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.*