CERT-PH Cybersecurity Threat Feeds

Issue Date	January 20, 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:

- FreakOut Malware Exploits Critical Bugs To Infect Linux Hosts
- FireEye Releases Tool For Auditing Networks For Techniques Used By SolarWinds Hackers
- Fourth Malware Strain Discovered In SolarWinds Incident
- DNSpooq Bugs Let Attackers Hijack DNS On Millions of Devices

- CRITICAL
- URGENT
- INFORMATION

Description

FreakOut Malware Exploits Critical Bugs to Infect Linux Hosts

2021.01.19 | Source(s): Bleeping Computer, Security Affairs, Threatpost

Analysis:

Security researchers uncovered a series of attacks associated with the FreakOut botnet that is targeting multiple unpatched flaws in applications running on top of Linux systems. The attacks observed aimed at devices that run one of the following products: TerraMaster TOS, Zend Framework and Liferay Portal. Botnet operators are actively scanning the internet for vulnerable applications affected by recently disclosed vulnerabilities and takeover the underlying Linux system. The flaws are identified as a RCE flaw in TerraMaster management panel (CVE-2020-28188), a deserialization flaw that affects the Zend Framework (CVE-2021-3007) and a Java unmarshalling flaw via JSONWS in Liferay Portal (CVE-2020-7961). The botnet could conduct multiple malicious activities such as delivering cryptocurrency miners, launching DDoS and spreading laterally across the company network.

Read more:

[https://securityaffairs[.]co/wordpress/113606/cyber-crime/freakout-botnet.html]
[https://www.bleepingcomputer[.]com/news/security/freakout-malware-exploits-critical-bugs-to-infect-linux-hosts/]
[https://threatpost[.]com/linux-attack-freakout-malware/163137/]

FireEye Releases Tool for Auditing Networks for Techniques Used by SolarWinds Hackers

2021.01.19 | Source(s): ZDNet

Analysis:

Cybersecurity firm FireEye has released a report detailing the techniques used by the SolarWinds hackers, also known as UNC2452, inside the networks of companies they breached. In addition to the report, researchers also released a free tool on GitHub, dubbed as Azure AD Investigator, that can help companies determine if the SolarWinds hackers used any of the techniques inside their networks. Some of the techniques used by the attackers includes, stealing the Active Directory Federation Services (AD FS) token-signing certificate and use it to forge tokens for arbitrary users (sometimes described as Golden SAML, modify or add trusted domains in Azure AD to add a new federated Identity Provider (IdP) that the attacker controls, compromise the credentials of on-premises user accounts that are synchronized to Microsoft 365 that have high privileged directory roles and highjacking an existing Microsoft 365 application by adding a rogue credential to it in order to use the legitimate permissions assigned to the application while bypassing MFA.

Read more:

[https://www.zdnet[.]com/article/multiple-backdoors-and-vulnerabilities-discovered-in-fiberhome-routers/]

Fourth Malware Strain Discovered in SolarWinds Incident

2021.01.19 | Source(s): ZDNet, Security Affairs

Analysis:

Security experts revealed that threat actors behind the SolarWinds supply chain attack leveraged a malware, dubbed as Raindrop, for lateral movement and deploying additional payloads. Raindrop is the fourth malware that was discovered during investigating the SolarWinds attack after the SUNSPOT backdoor, the Sunburst/Solorigate backdoor and the Teardrop tool. Raindrop is a loader that was used by attackers to deliver a Cobalt Strike payload. Raindrop is similar to the Teardrop tool, but while the latter was delivered by the initial Sunburst backdoor, the former was used for spreading across the victim's network.

Read more:

[https://securityaffairs[.]co/wordpress/113620/hacking/raindrop-solarwinds-attacks.html]
[https://www.zdnet[.]com/article/fourth-malware-strain-discovered-in-solarwinds-incident/]

DNSpooq Bugs Let Attackers Hijack DNS On Millions of Devices

2021.01.19 | Source(s): Bleeping Computer, Threatpost, ZDNet

Analysis:

Cybersecurity experts disclosed seven Dnsmasq vulnerabilities, collectively known as DNSpooq, that can be exploited to launch DNS cache poisoning, remote code execution, and denial-of-service attacks against millions of affected devices. Three of the DNSpooq vulnerabilities (tracked as CVE-2020-25686, CVE-2020-25684, CVE-2020-25685) allow for both DNS cache poisoning attacks, also known as DNS spoofing. Using this attack, threat actors can redirect users to malicious servers under their control, while to the visitors it appears as if they are visiting the legitimate site. This allows the attackers to perform phishing attacks, credential theft, or to distribute malware from what is perceived as a trusted company. The rest of the flaws are buffer overflow vulnerabilities tracked as CVE-2020-25687, CVE-2020-25683, CVE-2020-25682, and CVE-2020-25681 that could let attackers remotely execute arbitrary code on vulnerable networking equipment when Dnsmasq is configured to use DNSSEC.

Read more:

[https://www.bleepingcomputer[.]com/news/security/dnspooq-bugs-let-attackers-hijack-dns-on-millions-of-devices/]
[https://threatpost[.]com/dnspooq-flaws-allow-dns-hijacking-of-millions-of-devices/163163/]

CERT-PH Recommendations:

- **o** For Dnsmasq admins, until a patch is available, can temporarily disable DNSSEC validation option. Reduce the maximum queries allowed to be forwarded with the option--dns-forward-max=. Use protocols that provide transport security for DNS, such as DNS-over-HTTPS (D) or DoH).
- **o** Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Dnsmasq software -** version 2.83 or later
- **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.