CERT-PH Cybersecurity Threat Feeds

Issue Date	January 21, 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:

- Malwarebytes Says SolarWinds Hackers Accessed Its Internal Emails
- Bugs In Signal, Facebook, Google Chat Apps Let Attackers Spy On Users
- Hacker Leaks Full Database Of 77 Million Nitro PDF User Records
- Critical Cisco SD-WAN Bugs Allow RCE Attacks

- CRITICAL
- URGENT
- INFORMATION

Description

Malwarebytes Says SolarWinds Hackers Accessed Its Internal Emails

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

Analysis:

Malwarebytes discovered that the threat actor that coordinated the SolarWinds hack used applications with privileged access to infiltrate the company's Microsoft Office 365 and Azure environments. Malwarebytes does not use SolarWinds, but like many other companies, they were targeted by the same threat actor. According to researchers, after an extensive investigation, they determined that the attacker only gained access to a limited subset of internal company emails. Malwarebytes performed a deep investigation through its infrastructure, inspecting its source code, build and delivery processes, but it confirmed that internal systems showed no evidence of unauthorized access or compromise. This means that the customers of the security firm were not impacted using its anti-malware solution.

Read more:

[https://www.bleepingcomputer[.]com/news/security/malwarebytes-says-solarwinds-hackers-accessed-its-internal-emails/]
[https://securityaffairs[.]co/wordpress/113628/hacking/malwarebytes-solarwinds-attack.html]
[https://threatpost[.]com/malwarebytes-solarwinds-attackers/163190/]

Bugs in Signal, Facebook, Google Chat Apps Let Attackers Spy on Users

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

Analysis:

Vulnerabilities were found in multiple video conferencing mobile applications allowing attackers to listen to users' surroundings without permission before the person on the other end picked up the calls. Cybersecurity experts found the logic bugs in the Signal, Google Duo, Facebook Messenger, JioChat and Mocha messaging apps and are now fixed. However, before being patched, they made it possible to force targeted devices to transmit audio to the attackers' devices without the need of gaining code execution.

Read more:

[https://www.zdnet[.]com/article/multiple-backdoors-and-vulnerabilities-discovered-in-fiberhome-routers/]
[https://securityaffairs[.]co/wordpress/113657/hacking/signal-fb-messenger-logical-flaws.html]
[https://thehackernews[.]com/2021/01/google-discloses-flaws-in-signal-fb.html]

Hacker Leaks Full Database Of 77 Million Nitro PDF User Records

2021.01.20 | Source(s): Bleeping Computer

Analysis:

A stolen database containing the email addresses, names, and passwords of more than 77 million records of Nitro PDF service users was leaked today for free. The 14GB leaked database

contains 77,159,696 records with users' email addresses, full names, bcrypt hashed passwords, titles, company names, IP addresses, and other system-related information.

Read more:

[https://www.bleepingcomputer[.]com/news/security/hacker-leaks-full-database-of-77-million-nitro-pdf-user-records/]

Critical Cisco SD-WAN Bugs Allow RCE Attacks

2021.01.20 | Source(s): Bleeping Computer, Threat Post

Analysis:

Cisco has released security updates to address pre-auth remote code execution (RCE) vulnerabilities affecting multiple SD-WAN products and the Cisco Smart Software Manager software. Unauthenticated attackers can remotely exploit buffer overflow and command injection bugs to execute arbitrary code or to run arbitrary commands on the underlying operating system of devices running vulnerable releases of SD-WAN and Cisco Smart Software Manager Satellite software. The bugs include the SD-WAN Buffer Overflow, tracked as CVE-2021-1300 and pre-auth RCE vulnerabilities affecting Cisco's cloud licensing manager which are tracked as CVE-2021-1138, CVE-2021-1140, and CVE-2021-1142.

Read more:

[https://www.bleepingcomputer[.]com/news/security/cisco-fixes-critical-pre-auth-bugs-in-sd-wan-cloud-license-manager/]

[https://threatpost[.]com/critical-cisco-sd-wan-bugs-rce-attacks/163204/]

CERT-PH Recommendations:

o Users should switch to a unique and strong password that they don't use for any other website or online service.

o Using a password manager is also recommended as it helps manage and generate unique and for different sites.

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

- **Cisco Smart Software Manager Satellite** - version 6.3.0
- **Signal**
- **Google Duo**
- **Facebook Messenger**
- **JioChat**
- **Mocha**

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.