CERT-PH Cybersecurity Threat Feeds

Issue Date	January 27, 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:

- TikTok Bug Could Have Exposed Users' Profile Data and Phone Numbers
- Google fixes severe Golang Windows RCE vulnerability
- Windows NTLM Vulnerability Disclosed After Patch
- Unofficial Temporary Fix for Windows 10 NTFS Corruption Bug

- CRITICAL
- URGENT
- INFORMATION

Description

TikTok Bug Could Have Exposed Users' Profile Data and Phone Numbers

2021.01.26 | Source(s): Info Security, ZDNet

Analysis:

Security researchers disclosed a security flaw in TikTok that could have potentially enabled an attacker to build a database of the app's users and their associated phone numbers, which can be used for future malicious activities. The flaw resides in TikTok's "Find friends" feature that allows users to sync their contacts with the service to identify potential people to follow. An attacker can modifying the HTTP requests and automate the procedure of uploading and syncing contacts on a large scale and create a database of linked accounts and their connected phone numbers. Users who have linked a phone number with their account or logged in with a phone number is impacted by the flaw and a successful exploitation of it could have resulted in data leakage and privacy violation.

Read more:

[https://thehackernews[.]com/2021/01/tiktok-bug-could-have-exposed-users.html]
[https://www.infosecurity-magazine[.]com/news/tiktok-bug-gave-access-contacts/]

KindleDrip Exploit – Hacking A Kindle Device with A Simple Email

2021.01.26 | Source(s): Bleeping Computer

Analysis:

Google have fixed a severe remote code execution (RCE) vulnerability in the Go language (Golang), which could allow the execution of arbitrary code while building the malicious code on Windows. Tracked as CVE-2021-3115, the command injection and remote code execution flaw could allow attackers to fetch modules that make use of cgo, which can execute a gcc program from an untrusted download, when using the "go get" command. Google Published Go versions 1.14.14 (for 1.14.x and earlier), and 1.15.7 (for users of 1.15.x) to mitigate this vulnerability.

Read more:

[https://www.bleepingcomputer.com/news/security/google-fixes-severe-golang-windows-rce-vulnerability/]

Windows NTLM Vulnerability Disclosed After Patch

2021.01.25 | Source(s): Security Week

Analysis:

One of the vulnerabilities that Microsoft addressed on January 2021 Patch Tuesday could allow an attacker to relay NTLM authentication sessions and then execute code remotely. Tracked as CVE-2021-1678, the vulnerability has been described as an NT LAN Manager (NTLM) security feature bypass. The flaw could allow an attacker able to establish an NTLM session with a target machine can bind to the IRemoteWinspool interface and select the weak authentication level,

relay the NTLM authentication to the attacker's machine, and then execute remote procedure call commands.

Read more:
[https://www.securityweek[.]com/crowdstrike-discloses-details-recently-patched-windows-ntlm-vulnerability]

Unofficial Temporary Fix for Windows 10 NTFS Corruption Bug

2021.01.25 | Source(s): Bleeping Computer

Analysis:

Developers have released an unofficial fix for a Windows bug that could lead to the corruption of an NTFS volume by merely viewing a specially crafted file. Flaws in Windows 10 were discovered that allows non-privileged users to mark an NTFS volume as dirty, which could lead up to Windows displaying an error stating thats the drive was corrupted and prompt the user to reboot the computer to run chkdsk and fix the corruption. Security researchers have released an open-source filter driver which prevents the NTFS bug from being abused while waiting for an official fix from Microsoft.

Read more:
[https://www.bleepingcomputer.com/news/microsoft/windows-10-ntfs-corruption-bug-gets-unofficial-temporary-fix/?&web_view=true]

CERT-PH Recommendations:

o Update any vulnerable system/applications/devices to their latest and patched versions:
- **TikTok** – TikTok's latest version
- **Go -** versions 1.14.14 and 1.15.7
- **Microsoft System -** January Security Update

o Windows 10 users who experiences the operating system not starting properly can install the open-source filter driver while waiting for Microsoft to fix the bug.

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.