CERT-PH Cybersecurity Threat Feeds

Issue Date	February 04, 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:

- SolarWinds Patches Critical Vulnerabilities in The Orion Platform
- Cisco Fixes Critical Code Execution Bugs in SMB VPN Routers
- Critical Android Bugs Patched as Part of February Security Bulletin
- Dozen Chrome Extensions Caught Hijacking Google Search Results for Millions

- CRITICAL
- URGENT
- INFORMATION

Description

SolarWinds Patches Critical Vulnerabilities in The Orion Platform

2021.02.03 | Source(s): Bleeping Computer, Threastpost, The Hacker News

Analysis:

Researchers found three glaring vulnerabilities affecting the SolarWinds Orion platform, two of which are exploitable by a local attacker and the third one, most severe of all, allows a remote, unprivileged actor to take control of the Orion platform. The first flaw, tracked as CVE-2021-25274, exists in the collector service of the platform that relies heavily on Microsoft Message Queue (MSMQ), with a large list of unauthenticated private queues available. Successful exploitation may allow unauthenticated users to execute arbitrary code remotely. The second flaw discovered, tracked as CVE-2021-25275, was that the credentials for the Orion backend database were insufficiently protected and local users had unrestricted access to them. Lastly, the third flaw, tracked as CVE-2021-25276, exist in the SolarWinds Serv-U FTP Server, which if exploited, may allow an attacker with an admin account, to set the home directory to the root of the system drive and thus open the door to read or replace any file there.

Read more:

[https://www.bleepingcomputer[.]com/news/security/solarwinds-patches-critical-vulnerabilities-in-the-orion-platform/]
[https://threatpost[.]com/solarwinds-orion-bug-remote-code-execution/163618/]
[https://thehackernews[.]com/2021/02/3-new-severe-security-vulnerabilities.html]

Cisco Fixes Critical Code Execution Bugs in SMB VPN Routers

2021.02.03 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Cisco has addressed multiple pre-auth remote code execution (RCE) vulnerabilities affecting several small business VPN routers and allowing attackers to execute arbitrary code as root on successfully exploited devices. The security bugs with a severity rating of 9.8/10 were found in the web-based management interface of Cisco small business routers. According to security researchers, an attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device.

Read more:

[https://www.bleepingcomputer[.]com/news/security/solarwinds-patches-critical-vulnerabilities-in-the-orion-platform/]
[https://www.bleepingcomputer[.]com/news/security/cisco-fixes-critical-code-execution-bugs-in-smb-vpn-routers/]
[https://securityaffairs[.]co/wordpress/114192/hacking/smb-vpn-routers-issues.html]

Critical Android Bugs Patched as Part of February Security Bulletin

2021.02.03 | Source(s): Threatpost

Analysis:

Google patched five critical bugs in its Android operating system as part of its February Security Bulletin. Two of the flaws were remote code execution vulnerabilities found within the Android media framework

and system. Three additional critical Qualcomm bugs were reported by Google and patched by Qualcomm as part of a separate security bulletin disclosure. One of those flaws (CVE-2020-11163) has a Common Vulnerability Scoring System (CVSS) rating of 9.8 out of 10. The bug is tied to the wireless local area network (WLAN) chip used for Wi-Fi communications. In all, Google patched 22 vulnerabilities in the Android OS –15 of which included elevation-of-privilege (EOP) –class bugs. Another 22 security flaws were addressed by Qualcomm and impacted a range of device functions such as Wi-Fi radio, camera and device displays.

Read more:

[https://threatpost[.]com/five-critical-bugs-patched-feb-security-bulletin/163623/]

Dozen Chrome Extensions Caught Hijacking Google Search Results for Millions

2021.02.03 | Source(s): The Hacker News

Analysis:

A vast network of rogue extensions for Chrome and Edge browsers that were found to hijack clicks to links in search results pages to arbitrary URLs, including phishing sites and ads. Collectively known as CacheFlow, is a collection of 28 browser extensions in question that made use of a sneaky trick to mask its true purpose which is to leverage cache-control HTTP header as a covert channel to retrieve commands from an attacker-controlled server. Upon installation of an unsuspecting user, the extensions sent out analytics requests resembling Google Analytics to a remote server, which then beamed back a specially-crafted Cache-Control header containing hidden commands to fetch a second-stage payload that functioned as a downloader for the final JavaScript payload.

Read more:

[https://thehackernews[.]com/2021/02/over-dozen-chrome-extensions-caught.html]

CERT-PH Recommendations:

o Avoid installing unknown or unverified applications, especially from third-party distribution platforms. Scrutinize the application's permissions before installation and avoid allowing apps to view unnecessary information and other application's data.

o Users are urged to check their browser extensions and immediately remove the following extensions:

- **Direct Message for Instagram**
- **DM for Instagram**
- **Invisible mode for Instagram Direct Message**
- **Downloader for Instagram**
- **App Phone for Instagram**
- **Stories for Instagram**
- **Universal Video Downloader**
- **Video Downloader for FaceBook**
- **Vimeo Video Downloader**
- **Zoomer for Instagram and FaceBook**
- **VK UnBlock . Works fast.**
- **Odnoklassniki Unblock. Works quickly.**
- **Upload photo to Instagram**
- **Spotify Music Downloader**
- **The New York Times News**
- **FORBES**
- **Instagram Download Video & Image**
- **Vimeet Video Downloader**
- **Volume Controller**
- **Pretty Kitty, The Cat Pet**
- **Video Downloader for YouTube**
- **SoundCloud Music Downloader**
- **Instagram App with Direct Message DM**

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

- **Orion Platform - version 2020.2.4, Hotfix 1 for ServU-FTP 15.2.2.**

- **RV160 VPN Router** - version 1.0.01.02
- **RV160W Wireless-AC VPN Router** - version 1.0.01.02
- **RV260 VPN Router** - version 1.0.01.02
- **RV260P VPN Router with POE** - version 1.0.01.02
- **RV260W Wireless-AC VPN Router** - version 1.0.01.02
- **Android Firmware** - February Security Update

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.*