CERT-PH Cybersecurity Threat Feeds

Issue Date	February 11, 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:

- Apple Fixes SUDO Root Privilege Escalation Flaw in MacOS
- LodaRat Windows Malware Also Targets Android Devices
- Microsoft Urges Customers to Patch Critical Windows TCP/IP Bugs
- Intel Patches Tens of Vulnerabilities in Software, Hardware Products

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

Apple Fixes SUDO Root Privilege Escalation Flaw in MacOS

2021.02.09 | Source(s): Bleeping Computer

Analysis:

Apple has fixed a sudo vulnerability in macOS Big Sur, Catalina, and Mojave, allowing any local user to gain root-level privileges. Tracked as CVE-2021-3156, also known as Baron Samedit, is a SUDO vulnerability that may allow threat actors to gain root privileges on multiple Linux distributions, including Debian, Ubuntu and Fedora 33.

Read more:
[https://www.bleepingcomputer[.]com/news/apple/apple-fixes-sudo-root-privilege-escalation-flaw-in-macos/]

LodaRat Windows Malware Also Targets Android Devices

2021.02.10 | Source(s): The Hacker News

Analysis:

A previously known Windows remote access Trojan (RAT) with credential-stealing capabilities has now expanded its scope to set its sights on users of Android devices to further the attacker's espionage motives. Dubbed as Loda, is an AutoIt malware typically delivered via phishing lures that is equipped to run a wide range of commands designed to record audio, video and capture other sensitive information, with recent variants aimed at stealing passwords and cookies from browsers. The latest versions, dubbed as Loda4Android and Loda4Windows, are very similar and both come with a full set of data-gathering features that constitute a stalker application.

Read more:
[https://thehackernews[.]com/2021/02/lodarat-windows-malware-now-also.html]

Microsoft Urges Customers to Patch Critical Windows TCP/IP Bugs

2021.02.09 | Source(s): Bleeping Computer

Analysis:

Microsoft has urged customers today to install security updates for three Windows TCP/IP vulnerabilities rated as critical and high severity as soon as possible. The three TCP/IP security vulnerabilities impact computers running Windows client and server versions starting with Windows 7 and higher. Two of which expose unpatched systems to remote code execution (RCE) attacks, while the third one enables attackers to trigger a DoS state, taking down the targeted device. All of these attacks are all exploitable remote by unauthenticated attackers and are tracked as CVE-2021-24074, CVE-2021-24094, and CVE-2021-24086, respectively.

Read more:
[https://www.bleepingcomputer[.]com/news/security/microsoft-urges-customers-to-patch-critical-windows-tcp-ip-bugs/]

Intel Patches Tens of Vulnerabilities in Software, Hardware Products

2021.02.10 | Source(s): Security Week, Threatpost

Analysis:

Intel released updates that patch tens of vulnerabilities across many of the company's software and hardware products. The list of high-severity flaws includes a privilege escalation issue in the Intel Solid State Drive (SSD) Toolbox, and a denial-of-service (DoS) flaw in the XMM 7360 Cell Modem that can be exploited by an unauthenticated attacker who has network access. In its graphics drivers, Intel patched nearly two dozen vulnerabilities, including five high-severity bugs that can be exploited by authenticated attackers, four of which allow privilege escalation and one can be exploited for DoS attacks. Intel also informed customers about five vulnerabilities in Server Board, Server System and Compute Modules Baseboard Management Controller (BMC) products, including two high-severity privilege escalation issues. Medium-severity vulnerabilities have been patched in RealSense Depth Camera Manager (DCM), Ethernet I210 Controller series network adapters, Trace Analyzer and Collector, SOC Driver Package for STK1A32SC, Ethernet E810 adapter drivers for Linux and Windows, 722 Ethernet controllers, Software Guard Extensions (SGX), Extreme Tuning Utility (XTU), Quartus Prime software, PROSet/Wireless WiFi and Killer drivers for Windows 10, Enhance Privacy ID (EPID) SDK, Server Board Onboard Video driver for Windows, Collaboration Suite for WebRTC, and the Optane DC Persistent Memory installer for Windows. These security holes can lead to privilege escalation, DoS attacks and information disclosure, but exploitation in many cases requires a privileged user and local access.

Read more:
[https://www.securityweek[.]com/intel-patches-tens-vulnerabilities-software-hardware-products]
[https://threatpost[.]com/intel-graphics-driver-flaws/163810/]

CERT-PH Recommendations:

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 Avoid installing unknown or unverified applications, especially from third-party distribution platforms.

o Scrutinize the application's permissions before installation and avoid allowing apps to view unnecessary information and other application's data.

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

- **Microsoft February 2021 Monthly Patch**
- **Intel February Monthly 2021 Patch**
- **macOS Big Sur** - version 11.2
- **macOS Catalina** - version 10.15.7
- **macOS Mojave** - version 10.14.6

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.*