CERT-PH Cybersecurity Threat Feeds

Issue Date	April 14, 2021
TLP: White	

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:

- Adobe Fixes Critical Vulnerabilities in Photoshop And Digital Editions
- Microsoft April 2021 Patch Tuesday Fixes 108 Flaws Including 5 Zero-days
- Millions of Devices Impacted by NAME:WRECK Flaws
- New Linux, macOS Malware Hidden In Fake Browserify NPM Package

- CRITICAL
- URGENT
- INFORMATION

Description

Adobe Fixes Critical Vulnerabilities in Photoshop And Digital Editions

2021.04.13 | Source(s): Bleeping Computer, Threatpost

Analysis:

Adobe releases security updates to address a total of ten security vulnerabilities affecting Adobe Photoshop, Adobe Digital Editions, Adobe Bridge and RoboHelp. Among the four applications, Adobe Bridge has the most number of bugs fixed with four critical code execution bugs and two vulnerabilities rated as important. In addition to the vulnerabilities fixed in Adobe Bridge, Adobe also fixed two critical flaws in Adobe Photoshop, one critical vulnerability in Adobe Digital Editions and one important vulnerability in RoboHelp. Successful exploitation of these vulnerabilities could allow attackers to execute commands in Windows, installing of malware or even complete take over of the system.

Read more:

[https://www.bleepingcomputer[.]com/news/security/adobe-fixes-critical-vulnerabilities-in-photoshop-and-digital-editions/]
[https://threatpost[.]com/adobe-patches-critical-security-holes-bridge-photoshop/165371/]

Microsoft April 2021 Patch Tuesday Fixes 108 Flaws Including 5 Zero-days

2021.04.13 | Source(s): Bleeping Computer

Analysis:

Microsoft's Patch Tuesday fixed a total of 108 vulnerabilities 19 of which are rated as critical and 89 were rated as important. Included in the patch were five zero-day vulnerabilities, four of which were publicly disclosed vulnerabilities and one actively exploited in the wild. The four publicly disclosed vulnerabilities were RPC Endpoint Mapper Service Elevation of Privilege Vulnerability, Windows NTFS Denial of Service Vulnerability, Windows Installer Information Disclosure Vulnerability - PolarBear and Azure ms-rest-nodeauth Library Elevation of Privilege Vulnerability and are tracked as CVE-2021-27091, CVE-2021-28312, CVE-2021-28437 and CVE-2021-28458 respectively. Cybersecurity experts discovered a zero-day that is actively exploited in the wild, tracked as CVE-2021-28310, which is a Win32k Elevation of Privilege Vulnerability that could potentially allow an attacker escalation of privilege (EoP) that can be used together with other browser exploits to escape sandboxes or achieve system privileges. In addition to the zero-day vulnerabilities fixed, Microsoft also patched four critical remote code execution vulnerabilities that affect Microsoft Exchange products, tracked as CVE-2021-28480, CVE-2021-28481, CVE-2021-28482 and CVE-2021-28483.

Read more:

[https://www.bleepingcomputer[.]com/news/microsoft/microsoft-april-2021-patch-tuesday-fixes-108-flaws-5-zero-days/]

Millions of Devices Impacted by NAME:WRECK Flaws

2021.04.13 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Cybersecurity researchers disclosed nine vulnerabilities that affect implementations of the Domain Name System protocol in popular TCP/IP network communication stacks running on at least 100 million devices. Collectively tracked as NAME:WRECK, threat actors could exploit the vulnerabilities to deal significant damage to government or enterprise servers, healthcare facilities, retailers, or companies in the manufacturing business by stealing sensitive data, modifying or taking equipment offline for sabotage purposes. In addition, attackers could also tamper with critical building functions in residential or commercial locations to control heating and ventilation, disable security systems or tamper with automated lighting systems. The flaws were caused by lack of TXID validation, insufficiently random TXID and source UDP port, lack of domain name character validation, lack of label and name lengths validation, lack of NULL-termination validation, lack of the record count fields validation and lack of domain name compression pointer and offset validation.

Read more:

[https://www.bleepingcomputer.com/news/security/name-wreck-dns-vulnerabilities-affect-over-100-million-devices/]
[https://securityaffairs[.]co/wordpress/116734/reports/namewreck-flaws.html]

New Linux, macOS Malware Hidden in Fake Browserify NPM Package

2021.04.12 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Cybersecurity experts discovered a new malicious package in the npm registry that targets NodeJS developers using Linux and Apple macOS operating systems. Dubbed as web-browserify, the malicious package imitates the popular Browserify npm component downloaded over 160 million times over its lifetime. The package consists of a manifest file, package.json, a postinstall.js script, and an ELF executable called "run" present in a compressed archive, run.tar.xz within the npm component. Once installed, the scripts extract and launch the "run" Linux binary from the archive, which requests elevated or root permissions from the user. The extracted run binary is approximately 120 MB in size and has hundreds of legitimate open-source npm components bundled within it, that are being abused for malicious activities. Because elevated privileges would be requested almost at the same time "web-browserify" was being installed, the developer may be misled into believing that it is the legitimate installer activities requiring elevated permissions. The malware has advanced reconnaissance and fingerprinting capabilities, allowing it to collect bits of information from the infected system including system username, os information, information on Docker images, bluetooth-connected devices, virtual machines present on the system, CPU, RAM and hardware information.

Read more:

[https://www.bleepingcomputer[.]com/news/security/new-linux-macos-malware-hidden-in-fake-browserify-npm-package/

CERT-PH Recommendations:

- 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.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - Adobe Products:
    - Adobe Bridge - version 10.1.2 and 11.0.2 or later
    - Adobe Photoshop - 21.2.7 and 22.3.1 or later
    - Adobe Digital Editions - 4.5.11.187606 or later
    - Adobe RoboHelp - RH2020.0.4 or later
  - Microsoft April 2021 Patch
  - TCP/IP Stacks:
    - FreeBSD - latest version
    - Nucleus NET - latest version
    - NetX - latest version
- Security engineers can protect their systems from the NAME:WRECK vulnerabilities to develop signatures that detect DNS vulnerabilities such as:
  - Discover and inventory devices running the vulnerable stacks
  - Enforce segmentation controls and proper network hygiene

- Monitor progressive patches released by affected device vendors
- Configure devices to rely on internal DNS servers
- Monitor all network traffic for malicious packets

- 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.*