CERT-PH Cybersecurity Threat Feeds

Issue Date	April 15, 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:

- WhatsApp Bugs Allow Attackers to Remotely Hack Mobile Devices
- SAP Fixes Critical Bugs In Business Client, Commerce, and NetWeaver
- Second Google Chrome Zero-day Exploit
- NSA Discovers Critical Exchange Server Vulnerabilities

- CRITICAL
- URGENT
- INFORMATION

Description

WhatsApp Bugs Allow Attackers to Remotely Hack Mobile Devices

2021.04.14 | Source(s): Security Affairs, Hacker News

Analysis:

WhatsApp recently addressed two security vulnerabilities in its app for Android that could have been exploited by remote attackers to execute malicious code on a target device and potentially eavesdrop on communications. Tracked as CVE-2021-24027, the flaw stems from the implementation of content providers in Chrome, which is an IPC mechanism that is used by an application to share resources with any other application, and a same-origin policy bypass in the browser. Threat actors can trigger the issue by sending a specially-crafted HTML file to a victim via WhatsApp, which once opened in the victim's browser, executes the attacker's code contained in the HTML file. Successful exploitation may allow threat actors to perform a man-in-the-middle attack to achieve remote code execution or even exfiltrate the Noise protocol key pairs which are used to implement end-to-end encryption of user communications.

Read more:

[https://securityaffairs[.]co/wordpress/116833/hacking/whatsapp-flaws-remote-hack.html]
[https://thehackernews[.]com/2021/04/new-whatsapp-bug-couldve-let-attackers.html]

SAP Fixes Critical Bugs In Business Client, Commerce, and NetWeaver

2021.04.14 | Source(s): Bleeping Computer

Analysis:

The SAP Product Security Team shared information about vulnerabilities discovered and fixed in company products. In total, there are 19 security notes, five of them being updates to previous bugs. Tracked as CVE-2021-27602, the flaw is a remote code execution bug in SAP Commerce used to organize product information for distribution across multiple communication channels. With a critical rating of 9.8 out of 10, the flaw affects SAP Commerce 1808, 1811, 1905, 2005, and 2011. According to researchers, an attacker authorized into the Backoffice Product Content Management application of SAP Commerce can exploit it to achieve remote code execution on the system by injecting malicious code in the source rules.

Read more:

[https://www.bleepingcomputer[.]com/news/security/sap-fixes-critical-bugs-in-business-client-commerce-and-netweaver/]

Second Google Chrome Zero-day Exploit

2021.04.14 | Source(s): Bleeping Computer, Security Affairs

Analysis:

A second Chromium zero-day remote code execution exploit has been released on Twitter this week that affects current versions of Google Chrome, Microsoft Edge, and likely other Chromium-based browsers. According to cybersecurity experts, after disabling the sandbox, the exploit could launch Notepad on Google Chrome and Microsoft Edge. Moreover, the remote code execution vulnerability

could not escape Chromium's sandbox, which means that attackers have to chain them with a sandbox escape exploit to execute arbitrary code on the underlying system.
Read more:
[https://www.bleepingcomputer[.]com/news/security/second-google-chrome-zero-day-exploit-dropped-on-twitter-this-week/]
[https://securityaffairs[.]co/wordpress/116844/hacking/google-chromium-zero.html]

NSA Discovers Critical Exchange Server Vulnerabilities

2021.04.13 | Source(s): Bleeping Computer

Analysis:

Microsoft released security updates for Exchange Server that address a set of four vulnerabilities with severity scores ranging from high to critical. Tracked as CVE-2021-28480, CVE-2021-28481, CVE-2021-28482, and CVE-2021-28483, the flaws affect on-premise Exchange Server versions 2013 through 2019. Successful exploitation of these vulnerabilities may lead to remote code execution.
Read more:
[https://www.bleepingcomputer[.]com/news/security/nsa-discovers-critical-exchange-server-vulnerabilities-patch-now/]

CERT-PH Recommendations:

- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **WhatsApp** - version 2.21.4.18 or later
  - **SAP** - April 2021 Security Updates
  - **Google Chrome** - version 89.0.4389.128 or later
  - **Microsoft Exchange Server** - April 2021 Security Updates
- 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.*