CERT-PH Cybersecurity Threat Feeds

Issue Date	May 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 Reader Zero-day Vulnerability Exploited In The Wild
- Microsoft May 2021 Patch Tuesday Fixes 55 Flaws, 3 Zero-days
- Fake Chrome App Anchors Rapidly Worming 'Smish' Cyberattack
- Microsoft brings Threat and Vulnerability Management capability to Linux

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

Adobe Fixes Reader Zero-day Vulnerability Exploited In The Wild

2021.05.11 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Adobe released a massive Patch Tuesday security update that fixes vulnerabilities in twelve different applications, including one actively exploited vulnerability Adobe Reader. Tracked as CVE-2021-28550, is a remote code execution vulnerability that exists in Adobe Acrobat and Reader and could allow attackers to execute almost any command in Windows, including installing malware and the possibility of taking over the computer. In total, there were 43 vulnerabilities fixed, not including dependencies in Adobe Experience Manager. Out of all the Adobe security updates released, Adobe Acrobat & Reader had the most fixes, with 14 vulnerabilities.

Read more:

[https://www.bleepingcomputer[.]com/news/security/adobe-fixes-reader-zero-day-vulnerability-exploited-in-the-wild/]
[https://securityaffairs[.]co/wordpress/117792/security/windows-zero-day-4.html]

Microsoft May 2021 Patch Tuesday Fixes 55 Flaws, 3 Zero-days

2021.05.11 | Source(s): Bleeping Computer, ZDNet

Analysis:

Microsoft released May 2021 Patch Tuesday fixing 55 vulnerabilities four of which are classified as critical, 50 as important and one as moderate. Included in the patch are three zero-day vulnerabilities. The first zero-day, tracked as CVE-2021-31204, is an elevation of privilege vulnerability that impacts Microsoft's .NET and Visual Studio. The second vulnerability, tracked as CVE-2021-31207, is a security feature bypass vulnerability that affects Microsoft Exchange Server. Lastly, tracked as CVE-2021-31200, the third zero-day flaw is a remote code execution vulnerability that impacts Microsoft's Common Utilities, specifically Microsoft's NNI (Neural Network Intelligence) toolkit.

Read more:

[https://www.bleepingcomputer[.]com/news/microsoft/microsoft-may-2021-patch-tuesday-fixes-55-flaws-3-zero-days/]
[https://www.zdnet[.]com/article/microsofts-may-2021-patch-tuesday-55-flaws-fixed-four-critical/]

Fake Chrome App Anchors Rapidly Worming 'Smish' Cyberattack

2021.05.06 | Source(s): Threatpost

Analysis:

A new Android malware that impersonates the Google Chrome app has spread to hundreds of thousands of people. The fake app is being used as part of a sophisticated hybrid cyberattack campaign that also uses mobile phishing to steal credentials. According to researchers, the attack starts with a basic "smishing" gambit where targets receive an SMS text asking them to pay "custom fees" to release a package delivery. If they fall for it and click, a message comes up asking them to update the Chrome app. Once victims agree to that request, they're taken to a malicious website hosting the purported app. In reality, it's the malware, which is downloaded to their phones. According to security experts, the malware hides on mobile devices by using the official Chrome app’s icon and name, but its package, signature and version have nothing in common with the official app. In addition, attackers could easily tell the malware to steal other information on the device or detect when the user is logging into a corporate app or platform where they could steal valuable company data.

Read more:
[https://threatpost[.]com/fake-chrome-app-worming-smish-cyberattack/166038/]

Microsoft brings Threat and Vulnerability Management capability to Linux

2021.05.09 | Source(s): ZDNet

Analysis:

Microsoft is bringing its Threat and Vulnerability Management (TVM) q capabilities beyond Windows with support for macOS and Linux. TVM allows users to review recently discovered vulnerabilities within applications and potential misconfigurations across Linux and remediate any affected managed and unmanaged devices. Users currently can discover, prioritize and remediate more than 30 known unsecure configurations in macOS and Linux with this capability. Initially, Microsoft is supporting RHEL, CentOS and Ubuntu Linux, with Oracle Linux, SUSE and Debian being added shortly. The ability to assess secure configurations in threat and vulnerability management is a component of Microsoft Secure Score for Devices. It also will be part of Microsoft Secure Score all up once generally available.

Read more:
[https://www.zdnet[.]com/article/microsoft-brings-threat-and-vulnerability-management-capability-to-linux/]

CERT-PH Recommendations:

- 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.
- Users are urged to be cautious and check the email thoroughly before downloading and opening email attachments, especially when received from unknown email senders, as ransomware are usually found on email attachments and pirated application software.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Adobe Monthly Security Update** of May 2021
  - **Microsoft Monthly Security Update** ofac May 2021
- 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.*