CERT-PH Cybersecurity Threat Feeds

Issue Date	February 10, 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:

- Critical Firefox RCE Vulnerability Could be Chained with Other Bugs
- Adobe Fixes Critical Reader Vulnerability Exploited in The Wild
- Microsoft February 2021 Patch Tuesday Fixes 56 Flaws
- New BendyBear APT Malware Gets Linked to Chinese Hacking Group

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

Critical Firefox RCE Vulnerability Could be Chained with Other Bugs

2021.02.09 | Source(s): Security Week

Analysis:

Mozilla releases an update for Firefox 85 patches a critical information disclosure vulnerability that can be chained with other security flaws to achieve arbitrary code execution. The vulnerability is an information disclosure bug that exists within the implementation of the compressedTexImage3D API method in WebGL2. Exploitation requires the attacker to convince the targeted user to visit a malicious web page or open a malicious file. According to security researchers, the issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process.

Read more:
[https://www.securityweek[.]com/critical-firefox-vulnerability-can-allow-code-execution-if-chained-other-bugs]

Adobe Fixes Critical Reader Vulnerability Exploited in The Wild

2021.02.09 | Source(s): Bleeping Computer, Threatpost

Analysis:

Adobe has released a total of fifty security updates that affect seven of its products including Adobe Reader, Adobe Acrobat, Magento, Photoshop, Animate, Illustrator and Dreamweaver. Most notably, the update addresses an actively exploited vulnerability in Adobe Reader. Tracked as CVE-2021-21017, is a buffer overflow bug that would allow a malicious website to perform remote code execution on the vulnerable computer.

Read more:
[https://www.bleepingcomputer[.]com/news/security/adobe-fixes-critical-reader-vulnerability-exploited-in-the-wild/]
[https://threatpost[.]com/critical-adobe-windows-flaw/163789/]

Microsoft February 2021 Patch Tuesday Fixes 56 Flaws

2021.02.09 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Microsoft fixed a total of 56 vulnerabilities, with eleven classified as Critical, two as Moderate, and 43 as Important, with the release of February 2021 patch. The update included a fix for an actively exploited zero-day bug, tracked as CVE-2021-1732, which is a Windows Win32k elevation of privilege vulnerability that allows an attacker or malicious program to elevate their privileges to administrative privileges.

Read more:
[https://www.bleepingcomputer[.]com/news/security/microsoft-february-2021-patch-tuesday-fixes-56-flaws-1-zero-day/]
[https://securityaffairs[.]co/wordpress/114409/security/microsoft-february-2021-patch-tuesday.html]

New BendyBear APT Malware Gets Linked to Chinese Hacking Group

2021.02.09 | Source(s): Bleeping Computer

Analysis:

Security researchers shared information regarding a new polymorphic and highly sophisticated malware linked to a hacking group with known ties to the Chinese government. Dubbed as BendyBear, is malware whose shell code's only function is to be used to download other malicious payloads from attacker-controlled command and control (C2) servers. The malware has features and behavior that strongly resemble those of the WaterBear malware family which is connected to BlackTech, a cyberespionage group linked by threat researchers to the Chinese government.

Read more:
[https://www.bleepingcomputer[.]com/news/security/new-bendybear-apt-malware-gets-linked-to-chinese-hacking-group/]

CERT-PH Recommendations:

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

- **Fortinet Products**
- **FortiProxy SSL VPN**
- **FortiWeb**
- **FortiDeceptor**
- **Mozilla Firefox** - version 85.0.1

o To block attackers abusing Google Chrome's Sync API for harvesting and exfiltrating data from corporate environments, group policies are urged to create a list of approved CHrome extensions and block all others who haven't been checked for red flags.**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.*