CERT-PH Cybersecurity Threat Feeds

Issue Date	March 23, 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:

- RCE Flaw in Apache OFBiz Could Allow to Take Over the ERP System
- Adobe Addresses A Critical Vulnerability In ColdFusion Product
- Microsoft Exchange Servers Now Targeted By Black Kingdom Ransomware
- Popular Netop Remote Learning Software

- CRITICAL
- URGENT
- INFORMATION

Description

RCE Flaw in Apache OFBiz Could Allow to Take Over the ERP System

2021.03.22 | Source(s): Security Affairs, The Hacker News

Analysis:

The Apache Software Foundation fixed a high severity remote code execution flaw in Apache OFBiz that could have allowed attackers to take over the ERP system. Tracked CVE-2021-26295, the vulnerability exists due to an unsafe deserialization that occurs when malformed data or unexpected data could be used to abuse application logic, deny service, or execute arbitrary code when deserialized. This category of issue could compromise the availability, authorization process, and bypass access control. Successful exploitation of the vulnerability could allow unauthorized remote attackers to execute arbitrary code on the server and potentially take over the open-source ERP system.

Read more:

[https://securityaffairs[.]co/wordpress/115846/security/rce-flaw-apache-ofbiz-erp.html]
[https://thehackernews[.]com/2021/03/critical-rce-vulnerability-found-in.html]

Adobe Addresses A Critical Vulnerability In ColdFusion Product

2021.03.22 | Source(s): Security Affairs, Threatpost

Analysis:

Adobe has released security patches to address a critical vulnerability in Adobe ColdFusion that could be exploited by attackers to execute arbitrary code on vulnerable systems. Tracked as CVE-2021-21087, the flaw is caused by improper validation and can affect the control flow or data flow of a program, and allow for an attacker to launch a slew of malicious attacks. The vulnerability affects ColdFusion 2016 Update 16 and earlier versions, all ColdFusion 2018 Update 10, and earlier versions All ColdFusion 2021 Version 2021.0.0.323925.

Read more:

[https://securityaffairs[.]co/wordpress/115864/security/adobe-coldfusion-flaw.html]
[https://threatpost[.]com/adobe-critical-coldfusion-flaw-update/164946/]

Microsoft Exchange Servers Now Targeted by Black Kingdom Ransomware

2021.03.22 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts discovered a threat actor compromising Microsoft Exchange servers via the ProxyLogon vulnerabilities to deploy ransomware. Dubbed as Black Kingdom, the ransomware operation is exploiting the Microsoft Exchange Server ProxyLogon vulnerabilities to encrypt servers. According to the researchers, the threat actor exploits the ProxyLogon vulnerability to execute a PowerShell script that downloads the ransomware executable from 'yuuuuu44[.]com' and then pushes it out to other computers on the network. When encrypting devices, the ransomware will

encrypt files using random extensions and then create a ransom note named decrypt_file.TxT or in some cases, ReadMe.txt that uses slightly different text.**Read more:**
[https://www.bleepingcomputer[.]com/news/security/microsoft-exchange-servers-now-targeted-by-black-kingdom-ransomware/]

Popular Netop Remote Learning Software Vulnerabilities Disclosed

2021.03.22 | Source(s): ZDnet, The Hacker News

Analysis:

Cybersecurity experts disclosed the existence of multiple critical vulnerabilities in a remote student monitoring software Netop Vision Pro that a malicious attacker could abuse to execute arbitrary code and take over Windows computers. Netop Vision Pro is a software marketed for teachers to keep control of lessons. Features include viewing student screens and sharing the teachers', implementing web filters, pushing URLs, chat functions, and freezing student screens. The vulnerabilities were an incorrect privilege assignment problem, a default permissions error, the cleartext transmission of sensitive information, and authorization issues, tracked as CVE-2021-27192, CVE-2021-27193, CVE-2021-27194, and CVE-2021-27195, respectively. Altogether, the security flaws can be exploited to allow privilege escalation and remote code execution attacks within a compromised network.

Read more:
[https://www.zdnet[.]com/article/popular-remote-student-learning-program-found-to-be-riddled-with-security-holes/]
[https://thehackernews[.]com/2021/03/popular-netops-remote-learning-software.html]

CERT-PH Recommendations:

- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Apache OFBiz** - version 17.12.06 or later
  - **Adobe ColdFusion**
    - **2016 version** - Update 17 or later
    - **2018 version** - Update 11 or later
    - **2021 version** - 2021.0.0.323925 or later
  - **Microsoft Exchange Server** - March 2021 Security Updates
  - **Netop Vision and Netop Vision Pro** - version 9.7.2 or later
- Agencies mus 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.*