CERT-PH Cybersecurity Threat Feeds

Issue Date	May 06, 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:

- VMware Fixes Critical RCE Bug in vRealize Business For Cloud
- Cisco Bugs Allow Creating Admin Accounts and Executing Commands As Root
- New Pingback Malware Using ICMP Tunneling to Evade C&C Detection
- Banking Trojan Evolves from Distribution Through Porn to Phishing Schemes

- CRITICAL
- URGENT
- INFORMATION

Description

VMware Fixes Critical RCE Bug in vRealize Business for Cloud

2021.05.05 | Source(s): Bleeping Computer

Analysis:

VMware released security updates to address a critical severity vulnerability in vRealize Business for Cloud that enables unauthenticated attackers to remotely execute malicious code on vulnerable servers. VRealize Business for Cloud is an automated cloud business management solution designed to provide IT teams with cloud planning, budgeting, and cost analysis tools. Tracked as CVE-2021-21984, the vulnerability is a remote code execution vulnerability due to an unauthorized end point that impacts virtual appliances running VMware vRealize Business for Cloud prior to version 7.6.0. With a CVSS base score of 9.8, threat actors can exploit this security flaw using management interface (VAMI) upgrade APIs to gain access to unpatched vRealize Business for Cloud Virtual Appliances.

Read more:

[https://www.bleepingcomputer[.]com/news/security/vmware-fixes-critical-rce-bug-in-vrealize-business-for-cloud/]

Cisco Bugs Allow Creation of Admin Accounts and Executing Commands as Root

2021.05.05 | Source(s): Bleeping Computer

Analysis:

Cisco fixed critical SD-WAN vManage and HyperFlex HX software security flaws that could enable remote attackers to execute commands as root or create rogue admin accounts. Two of the vulnerabilities were an unauthorized message processing and privilege escalation vulnerability that impacts Cisco SD-WAN vManage Cluster Mode and were tracked as CVE-2021-1468 and CVE-2021-1505, respectively. The third flaw, tracked as CVE-2021-1497, is a command injection vulnerability that resides in Cisco HyperFlex HX Installer Virtual Machine. The vulnerabilities could enable unauthenticated, remote attackers to execute arbitrary code or access sensitive information. In addition, they could also be exploited locally by authenticated local attackers to gain escalated privileges or unauthorized access to an application vulnerable to attacks.

Read more:

[https://www.bleepingcomputer[.]com/news/security/cisco-bugs-allow-creating-admin-accounts-executing-commands-as-root/]

New Pingback Malware Using ICMP Tunneling to Evade C&C Detection

2021.05.04 | Source(s): The Hacker News

Analysis:

Cybersecurity researchers disclosed a novel malware that uses a variety of tricks to stay under the radar and evade detection, while stealthily capable of executing arbitrary commands on infected systems. Dubbed as Pingback, the Windows malware leverages Internet Control Message Protocol

(ICMP) tunneling for covert bot communications, allowing the adversary to utilize ICMP packets to piggyback attack code. Pingback ("oci.dll") achieves this by getting loaded through a legitimate service called MSDTC (Microsoft Distributed Transaction Coordinator) by taking advantage of a method called DLL search order hijacking, which involves using a genuine application to preload a malicious DLL file. Upon successful execution, Pingback resorts to using the ICMP protocol for its main communication. Pingback takes advantage of an Echo request (ICMP message type 8), with the message sequence numbers 1234, 1235, and 1236 denoting the type of information contained in the packet — 1234 being a command or data, and 1235 and 1236 being the acknowledgment for receipt of data on the other end. Some of the commands supported by the malware include the capability to run arbitrary shell commands, download and upload files from and to the attacker's host, and execute malicious commands on the infected machine.

Read more:

[https://thehackernews.com/2021/05/new-pingback-malware-using-icmp.html]

Banking Trojan Evolves from Distribution Through Pornographic to Phishing Schemes

2021.05.05 | Source(s): ZDNet

Analysis:

A banking Trojan focused on Brazilian targets has evolved from using pornography as a distribution model to phishing email models. Dubbed as Ousaban or Javali, the trojan is written in Delphi and is known for using sexual imagery as a lure and distribution vector. However, Ousaban has moved on since its roots in pornography and has now adopted a more typical approach in distribution. Phishing emails are sent using themes such as messages claiming there were failed package delivery attempts that ask users to open files attached to the email. The file contains an MSI Microsoft Windows installer package. If executed, the MSI extracts a JavaScript downloader that fetches a .ZIP archive containing a legitimate application which also installs the Trojan through DLL side-loading. In some cases, legitimate apps have been tampered with to fetch an encrypted injector that obtains a URL containing remote configuration files for a command-and-control (C2) server address and port, as well as another malicious file that changes various settings on a victim's PC. The trojan is capable of installing a backdoor, keylogging, screenshot capabilities, mouse and keyboard simulation, and the theft of user data.

Read more:

[https://www.zdnet[.]com/article/banking-trojan-evolves-from-distribution-through-porn-to-sophisticated-phishing-schemes/]

CERT-PH Recommendations:

- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **VMware vRealize Business for Cloud** - version 7.6.0
  - **Cisco SD-WAN vManage** - latest version
- 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.*