CERT-PH Cybersecurity Threat Feeds

Issue Date	March 31, 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 Bug Allowing Attackers To Steal Admin Credentials**
- **Researchers 2 Linux Kernel Flaws That Can Allow Bypassing Spectre Mitigations**
- **Reflected XSS Vulnerability Found In "Ivory Search" WP Plugin**
- **Flaws in Ovarro TBox RTUs Could Open Industrial Systems to Remote Attacks**

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

VMware Fixes Bug Allowing Attackers to Steal Admin Credentials

2021.03.30 | Source(s): Bleeping Computer, Security Affairs

Analysis:

VMware has published a security update addressing a high severity vulnerability in vRealize Operations that could allow attackers to steal admin credentials after exploiting vulnerable servers. Tracked as CVE-2021-21975, the vulnerability received a base score of 8.6 out of 10 and is caused by a Server Side Request Forgery bug in the vRealize Operations Manager API. Threat actors can exploit the vulnerability remotely without requiring authentications or user interaction in low complexity attacks to steal administrative credentials.

Read more:

[https://www.bleepingcomputer[.]com/news/security/vmware-fixes-bug-allowing-attackers-to-steal-admin-credentials/]
[https://securityaffairs[.]co/wordpress/116145/security/vmware-vrealize-operations-ssrf-flaw.html]

Researchers 2 Linux Kernel Flaws that can Allow Bypassing Spectre Mitigations

2021.03.29 | Source(s): Security Affairs, The Hacker News

Analysis:

Linux kernel fixed a couple of vulnerabilities that could allow an attacker to bypass mitigations designed to protect devices against Spectre attacks. Tracked as CVE-2020-27170, the flaw resides in the extended Berkeley Packet Filter (eBPF) technology. By default accessing the eBPF verifier is only accessible to privileged users with CAP_SYS_ADMIN, but a local user with the ability to insert eBPF instructions can use the eBPF verifier to abuse a Spectre like flaw to access all the content of the device's memory. The second vulnerability, tracked as CVE-2020-27171, also resides in the extended Berkeley Packet Filter (eBPF) technology. The issue triggers Integer underflow when restricting speculative pointer arithmetic allows unprivileged local users to leak the content of kernel memory and can be exploited to access contents from a 4Gb range of kernel memory.

Read more:

[https://securityaffairs[.]co/wordpress/116131/security/linux-kernel-flaws-spectre-bypass.html]
[https://thehackernews[.]com/2021/03/new-bugs-could-let-hackers-bypass.html]

Reflected XSS Vulnerability Found in "Ivory Search" WP Plugin

2021.03.30 | Source(s): Security Affairs-

Analysis:

Researchers discovered a reflected XSS vulnerability in the Ivory Search WordPress Plugin installed on over 60,000 sites that could be exploited by an attacker to perform malicious actions on a victim's website. According to researchers, a particular component on the Ivory Search plugin settings page was not validated properly which enabled the execution of malicious JavaScript code. The flaw is considered a medium severity vulnerability and affects Ivory search plugin version 4.6.0 and below.

Read more:
[https://securityaffairs[.]co/wordpress/116140/hacking/reflected-xss-ivory-search-wp-plugin.html]

Flaws in Ovarro TBox RTUs Could Open Industrial Systems to Remote Attacks

2021.03.29 | Source(s): The Hacker News

Analysis:

A total of five vulnerabilities have been discovered in Ovarro's TBox remote terminal units that could open the door for escalating attacks against critical infrastructures, like remote code execution and denial-of-service for vulnerable devices. The flaws detected include a vulnerability in its proprietary Modbus protocol used for communications that could be leveraged to run malicious code in TBox, crash a TBox system, and even decrypt the login password by capturing the network traffic between the RTU and the software tracked as CVE-2021-22646, CVE-2021-22642 and CVE-2021-22640 respectively. A fourth flaw, tracked as CVE-2021-22648, exists in the Modbus file access functions grants an attacker elevated permissions to read, alter or delete a configuration file.

Read more:
[https://thehackernews[.]com/2021/03/flaws-in-ovarro-tbox-rtus-could-open.html]

CERT-PH Recommendations:

- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **VMware vRealize Operations** - Security Patch
  - **Linux Kernel** - March Updates
  - **Ivory Search Wordpress Plugin** - version 4.6.1
  - **TBox Firmware** - version 1.46 or later
- 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.*