CERT-PH Cybersecurity Threat Feeds

Issue Date	February 16, 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:

- Siemens Patches 21 Vulnerabilities
- Researchers Link Russia's Sandworm APT to Attacks on Hosting Providers
- Facebook Phishing Campaign that Harvests Victim Credentials
- VMware Fixes Command Injection Issue In vSphere Replication

- CRITICAL
- URGENT
- INFORMATION

Description

Siemens Patches 21 Vulnerabilities

2021.02.09 | Source(s): Gov Info Security

Analysis:

Siemens has mitigated 21 vulnerabilities in two of its virtualization software tools that, if exploited, could enable attackers to gain remote control, exfiltrate data or cause systems to crash. All the vulnerabilities disclosed have a CVSS rank of 7.8. Siemens notes that the flaws, dubbed SSA-663999, are file parsing vulnerabilities that affect JT2Go, a 3D viewing tool, and Teamcenter, an enterprise visualization tool, in versions earlier than V13.1.0.1. The flaws come into play when the tools read files in formats such as PAR, BMP and TIFF, among others.

Read more:

[https://www.govinfosecurity[.]com/siemens-patches-21-vulnerabilities-in-2-tools-a-15983]

Researchers Link Russia's Sandworm APT to Attacks on Hosting Providers

2021.02.15 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Security researchers attribute a series of attacks targeting Centreon monitoring software used by multiple French organizations and attribute them to the Russia-linked Sandworm APT group. The first attack spotted dates back to the end of 2017 and the campaign continued until 2020. Threat actors mainly targeted IT service providers, particularly web hosting. The attackers used public and commercial VPN and anonymization services when connecting to the backdoors including the Tor network, EXpressVPN, VPNBook, and PrivateInternetAccess (PIA). The threat actors deployed a webshell on the compromised Centreon servers that were exposed on the internet, along with a backdoor dubbed as Exaramel. This backdoor is version 3.1.4. of the P.AS webshell, researchers found many similarities between this campaign and previous campaigns conducted by the Sandworm modus operandi.

Read more:

[https://securityaffairs[.]co/wordpress/114606/apt/anssi-sandworm-hosting-providers-attacks.html]
[https://www.bleepingcomputer[.]com/news/security/france-links-russian-sandworm-hackers-to-hosting-provider-attacks/]

Facebook Phishing Campaign that Harvests Victim Credentials

2021.02.15 | Source(s): Cybernews

Analysis:

Security researchers uncovered a phishing campaign on Facebook that tricked nearly 450,000 users in Germany since January. Dubbed as "Is that you", is a Facebook phishing campaign observed to be targeting UK users using identical tactics: sending a private Facebook message to unsuspecting users, claiming to have found a video or image with the victim featured in it. The message then leads the user through a chain of websites that have been infected with malicious scripts that harvest the victim's credential, and depending on their device, infect it with adware or other malware.

Read more:

[https://cybernews[.]com/security/facebook-phishing-campaign-spreading-to-uk]

VMware Fixes Command Injection Issue In vSphere Replication

2021.02.15 | Source(s): Security Affairs

Analysis:

VMware released security patches for a potentially serious vulnerability affecting the vSphere Replication product. Tracked as CVE-2021-21976, is a serious command injection vulnerability, with a CVSS base score of 7.2, that impacts vSphere Replication. The vulnerability can be exploited by an attacker with admin privileges to execute shell commands on the underlying system. VMware vSphere Replication is an extension to VMware vCenter Server that provides hypervisor-based virtual machine replication and recovery. vSphere Replication is an alternative to storage-based replication.

Read more:

[https://securityaffairs[.]co/wordpress/114619/security/vmware-command-injection-vsphere-replication.html]

CERT-PH Recommendations:

o 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.

o Be cautious on the following domains which are observed being used for scam campaigns:

- **hxxps://lapirixxx[.]xyz**
- **hxxp://blacksar[.]xyz**
- **hxxp://blacksar[.]in**
- **hxxp://blacksar[.]co**
- **hxxp://berafle[.]xyz**
- **hxxp://blacksar[.]date**
- **hxxp://blacksar[.]me**
- **hxxp://blacksar-dns[.]me**
- **hxxp://bendercrack[.]com**

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

- **JT2GO**
- **Teamcenter**
- **vSphere Replication**

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.*