CERT-PH Cybersecurity Threat Feeds

Issue Date	April 19, 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:

- Ryuk Ransomware Operation Updates Hacking Techniques
- Microsoft Fixes Windows 10 Bug That Can Corrupt NTFS Drives
- Russia-linked APT SVR Actively Targets These 5 Flaws
- Critical RCE Can Allow Attackers To Compromise Juniper Networks Devices

- CRITICAL
- URGENT
- INFORMATION

Description

Ryuk Ransomware Operation Updates Hacking Techniques

2021.04.17 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts observed that recent Ryuk ransomware attacks relied on compromising exposed Remote Desktop Protocol (RDP) connections to gain an initial foothold on a target network. In addition to the large-scale brute force and password spraying attacks against exposed RDP hosts to compromise user credentials, threat actors also used spear phishing techniques to distribute malware through malicious call centers that targeted corporate users and directed them to weaponized Excel documents. Moreover, threat actors also actively exploit two Windows vulnerabilities, a Win32k elevation of privilege vulnerability and a task scheduler elevation of privilege vulnerability. Tracked as CVE-2018-8453 and CVE-2019-1069, both flaws are patched and were rated with high severity of 7.8 and are exploited to increase permissions on a compromised machine.

Read more:

[https://www.bleepingcomputer[.]com/news/security/microsoft-fixes-windows-10-bug-that-can-corrupt-ntfs-drives/]

Microsoft Fixes Windows 10 Bug That Can Corrupt NTFS Drives

2021.04.17 | Source(s): Bleeping Computer

Analysis:

Microsoft fixed a flaw that could allow threat actors to create specially crafted downloads that crash Windows 10 simply by opening the folder where they are downloaded. Tracked as CVE-2021-28312, the bug was classified by Microsoft as a DDoS vulnerability and was titled as Windows NTFS Denial of Service Vulnerability. According to researchers, successful exploitation of the vulnerability could allow any user or program even with low privileges, to mark an NTFS drive as corrupted simply by accessing the special folder and could be used by threat actors to force a crash of a breached system to hide their malicious activity.

Read more:

[https://www.bleepingcomputer[.]com/news/security/microsoft-fixes-windows-10-bug-that-can-corrupt-ntfs-drives/]

Russia-linked APT SVR Actively Targets These 5 Flaws

2021.04.16 | Source(s): Security Affairs

Analysis:

Cybersecurity experts warn that the Russian-linked APT group SVR, also known as APT29, Cozy Bear and The Dukes), is actively exploiting five vulnerabilities in Fortinet, Zimbra, Pulse Secure, Citrix and VMware. Tracked as CVE-2018-13379, CVE-2019-9670, CVE-2019-11510, CVE-2019-19781 and CVE-2020-4006 respectively, the flaws were already addressed by their respective vendors however threat actors leverages these flaws to obtain login credentials and break into networks. According to the experts, this targeting and exploitation encompasses U.S. and allied networks, including national security and government-related systems.

Read more:

[https://securityaffairs[.]co/wordpress/116891/cyber-warfare-2/russia-svr-actively-targets-5-flaws.html]

Critical RCE Can Allow Attackers to Compromise Juniper Networks Devices

2021.04.16 | Source(s): Security Affairs

Analysis:

Cybersecurity provider Juniper Networks addressed a critical vulnerability that could be exploited by attackers to remotely hijack or disrupt vulnerable devices. Tracked as CVE-2021-0254, the flaw resides in the Junos OS and stems from the improper buffer size validation that can lead to a buffer overflow. According to security experts, successful exploitation may allow an unauthenticated remote attacker to send specially crafted packets to the device, triggering a partial Denial of Service (DoS) condition, or leading to remote code execution (RCE). In addition, an attacker could trigger the flaw to install a backdoor on a vulnerable device or to change its configuration

Read more:

[https://securityaffairs[.]co/wordpress/116907/security/juniper-networks-rce.html]

CERT-PH Recommendations:

- Users are urged to implement multi-factor authentication for RDP access. Perform network segmentation and controls to check SMB and NTLM traffic. Use the principle of least privilege and routine checks for account permissions.
- 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.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Microsoft Products** - April 2021 Patch
  - **Fortinet** - latest version
  - **Zimbra** - latest version
  - **Pulse Secure** - latest version
  - **Citrciix** - latest version
  - **VMware** - latest version
  - **Juniper Networks Junos OS** - 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.*