CERT-PH Cybersecurity Threat Feeds

Issue Date	March 25, 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:

- Cisco Addresses Critical Bug in Windows, MacOS Jabber Clients
- Microsoft Fixes Windows PSExec Privilege Elevation Vulnerability
- Hackers Leaked Details Of Millions Of Israeli Voters
- Multiple Vulnerabilities Found in GE Power Management Devices

- CRITICAL
- URGENT
- INFORMATION

Description

Cisco Addresses Critical Bug in Windows, MacOS Jabber Clients

2021.03.24 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Cisco has addressed a critical arbitrary program execution vulnerability impacting several versions of Cisco Jabber client software for Windows, macOS, Android, and iOS. Tracked as CVE-2021-1411, the flaw is caused by improper input validation of incoming messages' contents. The vulnerability was rated by Cisco with a 9.9/10 severity score. Successful exploitation could enable authenticated, remote attackers to execute arbitrary programs on Windows, macOS, Android or iOS devices running unpatched Jabber client software. Cisco Jabber is a web conferencing and instant messaging app that allows users to send messages via the Extensible Messaging and Presence Protocol (XMPP).

Read more:

[https://www.bleepingcomputer[.]com/news/security/cisco-addresses-critical-bug-in-windows-macos-jabber-clients/]

[https://securityaffairs[.]co/wordpress/115931/security/cisco-jabber-critical-flaw.html]

Microsoft Fixes Windows PSExec Privilege Elevation Vulnerability

2021.03.24 | Source(s): Bleeping Computer

Analysis:

Microsoft has fixed a vulnerability in the PsExec utility that allows local users to gain elevated privileges on Windows devices. PsExec is a Sysinternals utility designed to allow administrators to perform various activities on remote computers, such as launching executables and displaying the output on the local computer or creating reverse shells. According to cybersecurity researchers, threat actors commonly use PsExec in their post-exploitation toolkits to spread laterally to other machines on a network, execute commands on a large number of devices simultaneously, or deploy malware such as ransomware.

Read more:

[https://www.bleepingcomputer[.]com/news/security/microsoft-fixes-windows-psexec-privilege-elevation-vulnerability/]

Hackers Leaked Details of Millions Of Israeli Voters

2021.03.24 | Source(s): Security Affairs

Analysis:

Hackers have exposed personal and voter registration details of over 6.5 million Israeli voters, less than 24 hours before the election. According to researchers, the source of data seems to be the app, dubbed as Elector, developed by the software firm Elector Software for the Israeli political party Likud. Exposed files included names and ballot numbers of all 6,528,565 eligible voters and the personal details of over 3 Million Israeli citizens including full names, phone numbers, ID card numbers, home addresses, gender, age, and political preferences.

Read more:

[https://securityaffairs[.]co/wordpress/115918/hacking/israeli-voters-leak.html]

Multiple Vulnerabilities Found in GE Power Management Devices

2021.03.24 | Source(s): Security Affairs, Threatpost

Analysis:

Cybersecurity experts warn of vulnerabilities in GE Power Management Devices that could be exploited by an attacker to conduct multiple malicious activities on systems belonging to the Universal Relay (UR) family. The flaws could be exploited to access sensitive information, reboot the device, trigger a denial-of-service condition, and gain privileged access. The types of vulnerabilities affecting the devices are Inadequate Encryption Strength, Session Fixation, Exposure of Sensitive Information to an Unauthorized Actor, Improper Input Validation, Unrestricted Upload of File with Dangerous Type, Insecure Default Variable Initialization and Use of Hard-coded Credentials. The most severe issue, tracked as CVE-2021-27426, is a critical "Insecure Default Variable Initialization" rated with a CVSS score of 9.8 out of 10 and could be exploited by a remote attacker to bypass security restrictions.

Read more:

[https://securityaffairs[.]co/wordpress/115881/security/cisa-ge-power-management-devices-flaws.html]
[https://threatpost[.]com/cisa-security-flaws-ge-power-management/164961/]

CERT-PH Recommendations:

- 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:
  - **Cisco Jabber** - latest version
  - **Microsoft PsExec** - version 2.33 or later
  - **GE Universal Relay (UR) Products** - version 8.10 or later
- System administrators are advised to check wether the DTLS services of their servers are open and are publicly available in the Internet and implement necessary actions such as closing the port, if unused, and use anti-spoofing mechanism to remove the DTLS amplification vector.
- 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.*