CERT-PH Cybersecurity Threat Feeds

Issue Date	January 25, 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:

- Drupal Releases Fix for Critical Vulnerability with Known Exploits
- KindleDrip Exploit – Hacking A Kindle Device with A Simple Email
- SAP SolMan Exploit Released for Max Severity Pre-auth Flaw
- SonicWall Hacked Using Zero-Day Bugs in Its Own VPN Product

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

Drupal Releases Fix for Critical Vulnerability with Known Exploits

2021.01.22 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Drupal has released a security update to address a critical vulnerability in a third-party library with documented or deployed exploits available in the wild. Tracked as CVE-2020-36193, a vulnerability is caused by a bug in the PEAR Archive_Tar library used by the CMS. Successful exploitation allows an attacker to modify or delete all data and can also gain access to all non-public data available on the compromised server. Exploiting the Drupal vulnerability is only possible if the CMS is configured to allow and process .tar, .tar.gz, .bz2, or .tlz file uploads.

Read more:

[https://www.bleepingcomputer[.]com/news/security/drupal-releases-fix-for-critical-vulnerability-with-known-exploits/]
[https://securityaffairs[.]co/wordpress/113718/security/drupal-pear-archive_tar-library-flaw.html]

KindleDrip Exploit – Hacking A Kindle Device with A Simple Email

2021.01.22 | Source(s): Security Affairs

Analysis:

Amazon addressed a number of flaws affecting the Kindle e-reader that could have allowed an attacker to take control of victims' devices. The experts discovered three vulnerabilities that could be chained dubbed as KindleDrip exploit, by a remote attacker to execute code as root on the target's Kindle. The attacker only needs to know the email address associated with the device of the victim. The first vulnerability allowed an attacker to send an e-book to the victim's Kindle device. Then, the second vulnerability was used to run arbitrary code while the e-book is parsed, under the context of a weak user. The third vulnerability allows the attacker to escalate privileges and run code as root.

Read more:

[https://securityaffairs[.]co/wordpress/113743/hacking/kindle-kindledrip-exploit.html]

SAP SolMan Exploit Released for Max Severity Pre-auth Flaw

2021.01.22 | Source(s): Bleeping Computer, The Hacker News

Analysis:

Cybersecurity researchers have warned of a fully-functional exploit code which is now publicly available for a maximum severity pre-auth vulnerability impacting default configurations of an SAP Solution Manager (SolMan) component. Tracked as CVE-2020-6207, is a critical security flaw that is caused by a missing authentication check in the EEM Manager Solman component that could lead to the takeover of connected SAP systems. Successful exploitation could allow a remote unauthenticated attacker to expose virtually all of an organization's SAP applications, business process, and data to exfiltration or tampering, and will compromise all systems managed using the compromised SolMan instance.

Read more:
[https://thehackernews[.]com/2021/01/beware-fully-functional-released-online.html]
[https://www.bleepingcomputer[.]com/news/security/sap-solman-exploit-released-for-max-severity-pre-auth-flaw/]

SonicWall Hacked Using Zero-Day Bugs in Its Own VPN Product

2021.01.22 | Source(s): Hacker News, ZDnet

Analysis:

SonicWall reported that an attack occured leveraging zero-day vulnerabilities in its secure remote access products like NetExtender VPN client and Secure Mobile Access (SMA) that are utilized to provide customers with remote access to internal resources. According to the report, SonicWall's internal systems went down and the source code stored on the company's GitLab repository was accessed by threat actors. Patches for the zero-day vulnerabilities are not available at the time of writing, bu the they published a series of mitigations while they were investigating the incident and preparing for the upcoming patches.

Read more:
[https://threatpost[.]com/google-forms-set-baseline-for-widespread-bec-attacks/163223/]

CERT-PH Recommendations:

o Update any vulnerable system/applications/devices to their latest and patched versions:
  - Drupal - versions 9.1.3, 9.0.11, 8.9.13 and 7.78
  - SAP
  - Kindle Application

o Users of NetExtender VPN client and Secure Mobile Access are advised to check the advisory published by Sonicwall and apply necessary mitigation measures while waiting for the security patch

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.