CERT-PH Cybersecurity Threat Feeds

Issue Date	May 07, 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:

- **Qualcomm Vulnerability Impacts Nearly 40% Of All Mobile Phones**
- **Anti-Spam WordPress Plugin Could Expose Website User Data**
- **New Moriya Rootkit Used In The Wild To Backdoor Windows Systems**
- **New TsuNAME DNS Bug Allows Attackers to DDoS Authoritative DNS Servers**

- **CRITICAL**
- **URGENT**
- **INFORMATION**

Description

Qualcomm Vulnerability Impacts Nearly 40% Of All Mobile Phones

2021.05.06 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Cybersecurity experts discovered a high severity security vulnerability found in Qualcomm's Mobile Station Modem (MSM) chips that could enable attackers to access mobile phone users' text messages, call history, and listen in on their conversations. Tracked as CVE-2020-11292, the vulnerability could allow an attacker to use Android OS itself as an entry point to inject malicious and invisible code into phones. In addition, the flaw could also enable attackers to unlock the subscriber identification module (SIM) used by mobile devices to store network authentication info and contact information securely. According to security experts, malicious apps could also use the vulnerability to hide their activity under cover of the modem chip itself, effectively making themselves invisible to security features used by Android to detect malicious activity.

Read more:

[https://www.bleepingcomputer[.]com/news/security/qualcomm-vulnerability-impacts-nearly-40-percent-of-all-mobile-phones/]
[https://securityaffairs[.]co/wordpress/117620/security/qualcomm-bus-cve-2020-11292.html]

Anti-Spam WordPress Plugin Could Expose Website User Data

2021.05.05 | Source(s): Threatpost

Analysis:

Cybersecurity researchers detected an SQL-injection vulnerability in a WordPress plugin called "Spam protection, AntiSpam, FireWall by CleanTalk" that could expose user emails, passwords, credit-card data and other sensitive information to an unauthenticated attacker. Tracked as CVE-2021-24295, the flaw is caused by how the plugin performs filtering. It maintains a blocklist and tracks the behavior of different IP addresses, including the user-agent string that browsers send to identify themselves. The web-security vulnerability allows attackers to interfere with the queries that an application makes to its database, so that they intercept or infer the responses that databases return when queried. Prepared statements are one of the ways to prevent this as they isolate each query parameter so that an adversary would not be able to see the entire scope of the data that's returned.

Read more:

[https://threatpost[.]com/anti-spam-wordpress-plugin-expose-data/165901/]

New Moriya Rootkit Used In The Wild To Backdoor Windows Systems

2021.05.06 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Researchers detected an unknown threat actor using a new stealthy rootkit to backdoor targeted Windows systems in what looks like an ongoing espionage campaign dubbed TunnelSnake. Tracked as Moriya, the previously unknown malware is a passive backdoor that enables attackers to covertly spy on their victims' network traffic and send commands to compromised hosts. According to security experts, Moriya allowed TunnelSnake operators to capture and analyze incoming network traffic from the Windows kernel's address space, a memory region where the operating system's kernel resides and where typically only privileged and trusted code runs. In addition, threat actors used backdoored systems belonging to Asian and African diplomatic entities and other high-profile organizations to gain control of their networks and maintain persistence for months without being detected.

Read more:

[https://www.bleepingcomputer[.]com/news/security/new-moriya-rootkit-used-in-the-wild-to-backdoor-windows-systems/]
[https://securityaffairs[.]co/wordpress/117626/malware/moriya-rootkit-operation-tunnelsnake.html]

New TsuNAME DNS Bug Allows Attackers to DDoS Authoritative DNS Servers

2021.05.06 | Source(s): Bleeping Computer

Analysis:

A newly disclosed domain name server (DNS) vulnerability can be exploited by threat actors as an amplification vector in large-scale reflection-based distributed denial of service (DDoS) attacks targeting authoritative DNS servers. Dubbed as TsuNAME, the vulnerability affects DNSresolvers and can be exploited to attack authoritative servers. Resolvers vulnerable to TsuNAME will send non-stop queries to authoritative servers that have cyclic dependent records. Successful exploitation of the vulnerability may allow threat actors to carry out DDoS attacks against critical DNS infrastructure like large TLDs or ccTLDs, potentially affecting country-specific services.

Read more:

[https://www.bleepingcomputer[.]com/news/security/new-tsuname-dns-bug-allows-attackers-to-ddos-authoritative-dns-servers/]

CERT-PH Recommendations:

- To mitigate against TsuNAME, changes in the recursive resolver software must be implemented by including loop detection codes and caching cyclic dependent records. CycleHunter, an open source tool, can also reduce the impact of the flaw by preventing such events by detecting and pre-emptively fixing cyclic dependencies in the DNS zones.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Spam protection, AntiSpam, FireWall by CleanTalk** - version 5.153.4
- 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.*