June 10, 2024

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware PHP fixes critical RCE flaw impacting all versions for Windows.

Technical Details

A new PHP for Windows remote code execution (RCE) vulnerability has been disclosed, impacting all releases since version 5.x, potentially impacting a massive number of servers worldwide.

PHP is a widely used open-source scripting language designed for web development and commonly used on both Windows and Linux servers. The PHP project maintainers released a patch yesterday, addressing the vulnerability.

However, the application of security updates on a project with such a large-scale deployment is complicated and could potentially leave a significant number of systems vulnerable to attacks for extended periods.

Unfortunately, when a critical vulnerability impacting many devices is disclosed, threat actors and researchers immediately begin attempting to find vulnerable systems.

Such is the case with CVE-2024-4577, as The Shadowserver Foundation has already detected multiple IP addresses scanning for vulnerable servers.

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-4577
- https://www.bleepingcomputer.com/news/security/php-fixes-critical-rce-flaw-impacting-all-versions-for-windows/
- https://www.php.net/ChangeLog-8.php#8.3.8