New PHP Vulnerability Exposes Windows Servers to Remote Code Execution

Date: 10th June 2024 | Severity: High

Summary

A new critical security flaw impacting PHP that could be exploited to achieve remote code execution under certain circumstances.

Attack Vectors

- The vulnerability, tracked as CVE-2024-4577, has been described as a CGI argument injection vulnerability affecting all versions of PHP installed on the Windows operating system.
- "While implementing PHP, the team did not notice the Best-Fit feature of encoding conversion within the Windows operating system," security researcher Orange Tsai said.
- "This oversight allows unauthenticated attackers to bypass the previous protection of CVE-2012-1823 by specific character sequences. Arbitrary code can be executed on remote PHP servers through the argument injection attack."
- Following responsible disclosure on May 7, 2024, a fix for the vulnerability has been made available in PHP versions 8.3.8, 8.2.20, and 8.1.29.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Solution	• PHP versions of 8.1.29, 8.2.20 and 8.3.8 were released on June 6 to address this vulnerability. If you are unable to patch immediately, the DEVCORE blog does offer some mitigation guidance. As both PHP and DEVCORE note, CGI mode is insecure and dated, so it is recommended to migrate "to a more secure architecture."

Recommendation

- We strongly recommend that all installations running a version affected by the issues are upgraded to the latest version as soon as possible.
- Enable two factor authentication (2FA) which will deny malicious actors access to compromised accounts.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/06/new-php-vulnerability-exposes-windows.html
- https://www.tenable.com/blog/cve-2024-4577-proof-of-concept-available-for-php-cgi-argument-injection-vulnerability
- https://github.com/watchtowrlabs/CVE-2024-4577