Security Advisory 2024-058

Vulnerabilities in PHP

June 13, 2024 — v1.0

TLP:CLEAR

History:

- *13/06/2024 — v1.0 – Initial publication*

Summary

On June 6, 2024, a critical vulnerability was identified in certain versions of PHP that could allow the execution of arbitrary code or disclosure of sensitive information on Windows systems using Apache and PHP-CGI [1]. The vulnerability is currently being actively exploited, and several proof of concepts are available [2].

Technical details

The vulnerability, identified as **CVE-2024-4577**. with a CVSS score of 9.3 [3], affects certain PHP versions. When using Apache and PHP-CGI on Windows, if the system is configured to use specific code pages, Windows may utilise *Best-Fit* behaviour to replace characters in the command line given to Win32 API functions. This behaviour can cause the PHP CGI module to misinterpret these characters as PHP options, potentially allowing a malicious user to pass options to the PHP binary being executed. This vulnerability could lead to the exposure of script source code or the execution of arbitrary PHP code on the server.

Affected Products

The vulnerability affects PHP versions:

- 8.1.* before 8.1.29,
- 8.2.* before 8.2.20,
- 8.3.* before 8.3.8 when using Apache and PHP-CGI on Windows [1]

Recommendations

It is recommended to apply updates to the affected products as soon as possible.

References

[1] https://www.php.net/ChangeLog-8.php

[2] https://github.com/watchtowrlabs/CVE-2024-4577

[3] https://nvd.nist.gov/vuln/detail/CVE-2024-4577