Security Bulletin

CVE-2024-4577 - PHP CGI Argument Injection Vulnerability

Summary

First published: June 14, 2024

Description	In PHP versions earlier than 8.1 when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use “Best-Fit” behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.
Affected Products	enteliWEB
Recommended Action	NONE – enteliWEB is not affected
CVSS v3.0 Base Score	7.8 High
CVE ID	CVE-2024-4577

Risk

Scenario 1: If a web application uses php-cgi directly (indicating poor application architecture) and the server is using the affected PHP versions, the system can be exploited, allowing arbitrary code to be executed on remote PHP servers through an argument injection attack. This includes executing commands or running applications on the remote server.

Scenario 2: If a web application is poorly configured and PHP binaries are placed in a directory that permits the web server to execute CGI scripts, the server can also be exploited, enabling arbitrary code execution on remote PHP servers via the argument injection attack.

Why enteliWEB is not affected:

- enteliWEB employs a more secure architecture, using the FastCGI Module (Windows)
- enteliWEB configurations disable running any scripts outside of designated enteliWEB script folders. PHP and other binaries are not exposed to any web requests or direct access.

Summary: enteliWEB is not affected by **CVE-2024-4577**.