Security Bulletin for MiCC Enterprise PHP Argument Injection Vulnerability

Mitel

OVERVIEW

This security bulletin provides product-specific details on the vulnerabilities described in Mitel Security Advisory 24-0018. Visit http://www.mitel.com/security-advisories for more details.

This Security Bulletin provides details and recommended solutions to address a PHP Argument Injection Vulnerability in MiCC Enterprise.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSION(S) AFFECTED	SOLUTION(S) AVAILABLE
MiCC Enterprise	9.7 SP1 and earlier	See KMS article SO8099 for instructions.

RISK / EXPOSURE

PHP Argument Injection Vulnerability (CVE-2024-4577)

MiCC Enterprise versions 9.7 SP1 and earlier utilize the vulnerable PHP scripting engine and may be affected by the PHP Argument Injection Vulnerability, which could allow an unauthenticated attacker to conduct an argument injection attack. A successful exploit of this vulnerability could allow a malicious user to pass options to the PHP binary being run and thus reveal the source code of scripts and run arbitrary PHP code on the server.

The PHP Argument Injection vulnerability may only be exploited if the web server is running on Windows. This is because the root cause involves how Windows converts certain string characters, depending on the locale setting. Additionally, the web server must be running a vulnerable version of the PHP scripting engine. PHP scripting must also be exposed by the web server via the CGI mechanism or by exposing the PHP binary, which is the default configuration in XAMPP.

The vulnerability severity is rated as **Critical**.

MITIGATION / WORKAROUNDS

Customers with affected MiCC Enterprise versions are encouraged to consult the Knowledge Management System (KMS) article for mitigation instructions.

SOLUTION INFORMATION

Mitel has provided user instructions that address this vulnerability for MiCC Enterprise versions 9.7 SP1 and earlier.

Please see Mitel Knowledge Base article KB000116874, MiCC Enterprise ACD vulnerability, CVE-2024-4577.

If you do not have access to this link, please contact your Mitel Authorized Partner for support.

For further information, please contact Mitel Product Support.

REVISION HISTORY

Version	Date	Description
1.0	2024-07-10	Initial version