July 11, 2024

Overall Rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a recently released update by Mitel security advisories to address critical vulnerabilities in the following products:

- Mitel MiContact Center Enterprise – version 9.7 SP1 and prior
- Mitel CMG Suite – version 9.0 and prior
- Unify OpenScape Voice Trace Manager – version V8.R0.9.13 and prior

Technical Details

CVE-2024-4577: In 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, 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.

OpenScape Voice Trace Manager version OSV-TM V8 R0.9.13 and earlier utilizes the vulnerable PHP scripting engine and may be affected by 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.

Based on the available information, 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.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist 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 at vulnerabilityandriskmanagement@gov.bc.ca

References

- **CVE-2024-4577**
- Mitel security advisory - 24-0018
- Mitel security advisory - OBSO-2407-01
- Mitel Security Advisories