Security Bulletin for Mitel MiCollab

SECURITY BULLETIN ID: 24-0021-001

RELEASE VERSION: 3.0

DATE: 2024-08-13

OVERVIEW

This security bulletin provides product-specific details on the vulnerabilities described in Mitel Security Advisory 24-0021. Visit http://www.mitel.com/security-advisories for more details.

This Security Bulletin provides details and recommended solutions to address a command injection vulnerability found in the MiCollab Client Server of Mitel MiCollab and MiVB SVI.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSION(S) AFFECTED	SOLUTION(S) AVAILABLE
MiCollab	9.8 SP1 (9.8.1.5) and earlier	Upgrade to MiCollab 9.8 SP1 FP1 (9.8.1.108) or later. Alternative Solution: Mitel provided script available for releases 9.7, 9.7 SP1, 9.8 and 9.8 SP1. Consult the KMS article for more details.
MiVB SVI	1.0.0.27 and earlier	Following the instructions found in the KMS article.

RISK / EXPOSURE

Command Injection Vulnerability (CVE-2024-41714)

A command injection vulnerability in the MiCollab Client Server of Mitel MiCollab and MiVB SVI could allow an authenticated attacker to conduct a command injection attack due to insufficient validation of user input.

A successful exploit of this vulnerability could allow an attacker with access to the MiCollab Client Web Interface and MiCollab Desktop Client Application to execute arbitrary commands with elevated privileges within the context of the MiCollab system, with potential impacts on the confidentiality, integrity, and availability of the system.

The risk due to this vulnerability is rated as **Critical**.

Mitel
Powering connections

	CVSS v3.1
CVSS OVERALL SCORE:	9.9
CVSS VECTOR:	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
CVSS BASE SCORE:	9.9
CVSS TEMPORAL SCORE:	Not Defined
CVSS ENVIRONMENTAL SCORE:	Not Defined
OVERALL RISK LEVEL:	Critical

MITIGATION / WORKAROUNDS

Customers with affected product versions should upgrade to the highlighted solution versions or later. The risk may be mitigated by following the instructions found in the KMS article.

SOLUTION INFORMATION

This issue is corrected in MiCollab 9.8 SP1 FP1 (9.8.1.108). Customers are advised to upgrade to this or subsequent releases.

Mitel has also made available a script that addresses this vulnerability for MiCollab releases 9.7, 9.7 SP1, 9.8 and 9.8 SP1. Upgrade to these releases and apply the provided fix or upgrade to a later release.

Please see Mitel Knowledge Base article KB000116725, “MiCollab Security Update - CVE-2024-41714 Command Injection Vulnerability”

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	2024-07-24	Initial version
2.0	2024-07-29	Updated the available solutions
3.0	2024-08-13	Updated the available solutions

Mitel
Powering connections