Security Bulletin for Mitel MiCollab Access Control Vulnerability

SECURITY BULLETIN ID: 22-0001-001

RELEASE VERSION: 2.0

DATE: 2022-03-11

OVERVIEW

This security bulletin provides product-specific details on the vulnerabilities described in Mitel Security Advisory 22-0001. Visit http://www.mitel.com/security-advisories for more details.

This Security Bulletin provides details and recommended solutions to address a security access control vulnerability in the Mitel MiCollab application.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSIONS(S) AFFECTED	SOLUTIONS(S) AVAILABLE
Mitel MiCollab	Prior to and including 9.4 SP1	Upgrade to R9.4 SP1 FP1 For earlier releases, Mitel provided script available for releases R8.0 SP2 FP4 to R9.4 SP1 and mitigation for R5.0 to R8.0 SP2 FP3

RISK / EXPOSURE

Security access control vulnerability (CVE-2022-26143)

A security access control vulnerability in Mitel MiCollab may allow a remote unauthenticated attacker to gain unauthorized access to sensitive information and services, potential code execution in the context of the conference component and impact the performance of the affected system. In the case of a sustained denial of service attack through a series of malformed messages, improper message handling may cause the MiCollab system to generate significant outbound traffic that does not include sensitive information.

The vulnerability is rated as critical for MiCollab deployments in Server-Gateway mode without firewall protection. The severity is rated high for MiCollab deployments on protected internal networks.

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

Mitel
Powering connections

	CVSS v3.1
CVSS OVERALL SCORE:	9.4
CVSS VECTOR:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H
CVSS BASE SCORE:	9.4
CVSS TEMPORAL SCORE:	Not Defined
CVSS ENVIRONMENTAL SCORE:	Not Defined
OVERALL RISK LEVEL:	Critical

MITIGATION / WORKAROUNDS

Available mitigation to reduce external exposure includes:

- Configuration change to deploy MiCollab on an internal network, protected by MiVoice Border Gateway or appropriately configured firewall
- Apply firewall rules to block specific ports to the MiCollab (*see KMS article)*.

Mitel has made available a script that provides mitigation for this vulnerability.

Please see Mitel Knowledge Base article SO6795, Security Access Control Remediation for MiCollab and MiVoice Business Express Servers https://mitel.custhelp.com/app/answers/answer_view/a_id/1017561. 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.

SOLUTION INFORMATION

This issue is addressed in MiCollab R9.4 SP1 FP1. Customers are advised to upgrade to this release.

For further information, please refer to the Mitel Knowledge Base article listed above or contact Mitel Product Support.

REVISION HISTORY

Version	Date	Description
1.0	2022-02-22	Initial version
2.0	2022-03-11	Updated with CVE identifier, solution release information, and updated mitigation release information.

Mitel
Powering connections