Security Bulletin for Mitel MiCollab

⋈ Mitel®

OVERVIEW

This security bulletin provides product-specific details on the vulnerabilities described in Mitel Security Advisory 24-0016. Visit http://www.mitel.com/security-advisories for more details.

This Security Bulletin provides details and recommended solutions to address a privilege escalation vulnerability found in the MiCollab desktop client of Mitel MiCollab and MiVoice Business Solution Virtual Instance (MiVB SVI).

Credit is given to Julian Horoszkiewicz of the Eviden Red Team for the discovery.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSION(S) AFFECTED	SOLUTION(S) AVAILABLE
MiCollab	9.7.1.110 and earlier	Upgrade to MiCollab 9.8 or later. See KMS article for instructions.
MiVoice Business Solution Virtual Instance (MiVB SVI)	1.0.0.25	Upgrade available for the affected component. See KMS article for instructions.

RISK / EXPOSURE

Privilege Escalation Vulnerability (CVE-2024-35315)

A privilege escalation vulnerability in the MiCollab desktop client of Mitel MiCollab and MiVoice Business Solution Virtual Instance (MiVB SVI) could allow an authenticated attacker to conduct a privilege escalation attack due to improper file validation.

A successful exploit of this vulnerability could allow an attacker to run arbitrary code with elevated privileges, with potential impacts on the confidentiality, integrity, and availability of the system.

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

	CVSS v3.1
CVSS OVERALL SCORE:	7.8
CVSS VECTOR:	AV:L/AC:L/PR:L/UI:N/S:U/ C:H/I:H/A:H
CVSS BASE SCORE:	7.8
CVSS TEMPORAL SCORE:	Not Defined
CVSS ENVIRONMENTAL SCORE:	Not Defined
OVERALL RISK LEVEL:	High

MITIGATION / WORKAROUNDS

Customers with affected MiCollab versions should upgrade to the highlighted solution versions or later.

As an alternative, the MiCollab desktop client application can be updated to version 9.8. The MiCollab Client 9.8 for Windows desktops is fully compatible with the MiCollab 9.7.1.110 server. Refer to the KMS article for installation instructions.

Customers using the MiVoice Business Solution Virtual Instance (MiVB SVI) are encouraged to consult the Knowledge Management System (KMS) article for installation instructions.

SOLUTION INFORMATION

These issues are corrected in MiCollab 9.8 or later. Customers are advised to upgrade to this or subsequent releases.

Please see Mitel Knowledge Base article KB000116728, "MiCollab Security Update, CVE-2024-35315"

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	2024-05-23	Initial version
2.0	2024-06-05	Updated the available solutions