Security Bulletin for Mitel MiCollab

Mitel

OVERVIEW

This security bulletin provides product-specific details on the vulnerabilities described in Mitel Security Advisory 24-0023. 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 NuPoint Unified Messaging (NPM) component of MiCollab.

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 release 9.8 and 9.8 SP1. Consult the KMS article for more details.

RISK / EXPOSURE

Privilege Escalation Vulnerability (CVE-2024-35287)

A privilege escalation vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab could allow an authenticated attacker with administrative privilege to conduct a privilege escalation attack due to the execution of a resource with unnecessary privileges.

A successful exploit of this vulnerability could allow an attacker with local access to execute arbitrary commands 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**.

Mitel
Powering connections

CVSS v3.1	
CVSS OVERALL SCORE:	8.2
CVSS VECTOR:	AV:L/AC:L/PR:H/UI:N/S:C/ C:H/I:H/A:H
CVSS BASE SCORE:	8.2
CVSS TEMPORAL SCORE:	Not Defined
CVSS ENVIRONMENTAL SCORE:	Not Defined
OVERALL RISK LEVEL:	High

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.

Please see Mitel Knowledge Base article KB000116784, "MiCollab Security Update CVE-2024-35287 - Privilege Escalation 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