Security Bulletin for MiVoice Business Express Access Control Vulnerability

SECURITY BULLETIN ID: 22-0001-002

RELEASE VERSION: 1.0

DATE: 2022-02-22

Mitel®

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 MiVoice Business Express.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSIONS(S) AFFECTED	SOLUTIONS(S) AVAILABLE
MiVoice Business Express	Prior to and including R8.1	Mitel provided script available for releases R8.0 and R8.1

RISK / EXPOSURE

Security access control vulnerability

A security access control vulnerability in MiVoice Business Express 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 MiVoice Business Express system to generate significant outbound traffic that does not include sensitive information.

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

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

	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 MiVoice Business Express on an internal network, protected by MiVoice Border Gateway or appropriately configured firewall
- Apply firewall rules to block specific ports to the MiVoice Business Express (*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

For further information, please contact Mitel Product Support.

REVISION HISTORY

Version	Date	Description
1.0	2022-02-22	Initial version

Mitel
Powering connections