Security Bulletin for MiContact Center Business

SECURITY BULLETIN ID: 24-0011-001

RELEASE VERSION: 2.0

DATE: 2024-05-23

Mitel

OVERVIEW

This security bulletin provides product-specific details on the vulnerabilities described in Mitel Security Advisory 24-0011. Visit http://www.mitel.com/security-advisories for more details.

This Security Bulletin provides details and recommended solutions to address a stored cross-site scripting (XSS) vulnerability found in the MiContact Center Business.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSION(S) AFFECTED	SOLUTION(S) AVAILABLE
MiContact Center Business	10.0.0.4 Hotfix KB560110 and earlier	Upgrade to MiContact Center Business version 10.1.0.1, OR; Mitel has provided hotfixes KB560730 and KB560732 that are available for releases 10.0.0.4 and 9.5.0.3, respectively. Upgrade to one of these releases and apply the provided hotfix or upgrade to a later release.

These issues only impact deployments using the legacy chat component.

RISK / EXPOSURE

Stored Cross-Site Scripting (XSS) Vulnerability (CVE-2024-35283)

A stored cross-site scripting (XSS) vulnerability in the Ignite component of the MiContact Center Business could allow an unauthenticated attacker to conduct a stored cross-site scripting (XSS) attack due to insufficient input validation.

A successful exploit of this vulnerability could allow an attacker to execute arbitrary scripts.

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

Mitel
Powering connections

	CVSS v3.1
CVSS OVERALL SCORE:	9.3
CVSS VECTOR:	AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N
CVSS BASE SCORE:	9.3
CVSS TEMPORAL SCORE:	Not Defined
CVSS ENVIRONMENTAL SCORE:	Not Defined
OVERALL RISK LEVEL:	Critical

MITIGATION / WORKAROUNDS

The risk may be mitigated by turning off the Legacy Chat or converting to CloudLink Contact Center Messenger Chat.

SOLUTION INFORMATION

These issues are corrected in MiContact Center Business version 10.1.0.1. Customers are advised to upgrade to this or a subsequent release.

Mitel has also made available hotfixes KB560730 and KB560732 that addresses this vulnerability for MiContact Center Business releases 10.0.0.4 and 9.5.0.3, respectively. Upgrade to this release and apply the provided hotfix or upgrade to a later release.

Please see Mitel Knowledge Base article KB000117907 "MiContact Center Business - Security update, CVE-2024-35283 and CVE-2024-35284"

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	2024-04-24	Initial version
2.0	2024-05-23	Updated the CVE Number

Mitel
Powering connections