Security Bulletin for Mitel 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit

SECURITY BULLETIN ID: 24-0006-001

RELEASE VERSION: 2.0

DATE: 2024-04-25

OVERVIEW

This security bulletin provides product-specific details on the vulnerabilities described in Mitel Security Advisory 24-0006. Visit http://www.mitel.com/security-advisories for more details.

This Security Bulletin provides details and recommended solutions to address a buffer overflow vulnerability found in the 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit.

Credit is given to Kevin Joensen of CSIS for the discovery.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSION(S) AFFECTED	SOLUTION(S) AVAILABLE
Mitel 6800 Series SIP Phones	Version 6.3 SP3 HF4 and earlier	Upgrade to version 6.4 or later
Mitel 6900 Series SIP Phones	Version 6.3 SP3 HF4 and earlier	Upgrade to version 6.4 or later
Mitel 6900 Series SIP Phones	Version 6.3.3 and earlier	Upgrade to version 6.4 or later
Mitel 6970 Conference Unit	Version 5.1.1 SP8 and earlier	Upgrade to version 6.4 or later

RISK / EXPOSURE

Buffer Overflow Vulnerability (CVE-2024-31963)

A buffer overflow vulnerability in the 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit could allow an authenticated attacker with network access to conduct a buffer overflow attack due to insufficient bounds checking and input sanitization.

A successful exploit could allow an attacker to gain access to sensitive information, modify system configuration or execute arbitrary commands within the context of the system, with potential impact to the confidentiality, integrity, and availability of the phone.

Mitel
Powering connections

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

	CVSS v3.1
CVSS OVERALL SCORE:	7.5
CVSS VECTOR:	AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE:	7.5
CVSS TEMPORAL SCORE:	Not Defined
CVSS ENVIRONMENTAL SCORE:	Not Defined
OVERALL RISK LEVEL:	High

Mitel has recently disclosed several vulnerabilities which, if exploited in combination result in increased risk. Customers are strongly advised to update to the solution version as soon as feasible or apply the available mitigations.

MITIGATION / WORKAROUNDS

The risk may be mitigated by following the instructions found in the KMS article.

SOLUTION INFORMATION

These issues are corrected in Mitel 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit, versions 6.4 or later. Customers are advised to upgrade to this or a subsequent release.

Please see Mitel Knowledge Base article KB000117967, “Mitel 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit Security Update, CVE-2024-31963”

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	2024-04-17	Initial version
2.0	2024-04-25	Updated the Risk/Exposure section

Mitel
Powering connections