

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

SECURITY BULLETIN ID: 24-0009-001

RELEASE VERSION: 2.0

DATE: 2024-04-25



OVERVIEW

This security bulletin provides product-specific details on the vulnerabilities described in Mitel Security Advisory 24-0009. Visit <http://www.mitel.com/security-advisories> for more details.

This Security Bulletin provides details and recommended solutions to address an argument injection 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

Argument Injection Vulnerability (CVE-2024-31966)

An argument injection vulnerability in the 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit could allow an authenticated attacker with administrative privilege and physical access to conduct an unauthorized access attack due to insufficient parameter sanitization.

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

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

CVSS v3.1**CVSS OVERALL SCORE:** 6.2**CVSS VECTOR:** AV:P/AC:L/PR:H/UI:N/S:U/
C:H/I:H/A:H**CVSS BASE SCORE:** 6.2**CVSS TEMPORAL SCORE:** Not Defined**CVSS ENVIRONMENTAL SCORE:** Not Defined**OVERALL RISK LEVEL:** Medium**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 [KB000117973](#), "Mitel 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit Security Update, CVE-2024-31966"

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