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

SECURITY BULLETIN ID: 24-0019-001

RELEASE VERSION: 2.0

DATE: 2024-07-30

OVERVIEW

This security bulletin provides product-specific details on the vulnerabilities described in Mitel Security Advisory 24-0019. Visit http://www.mitel.com/security-advisories for more details.

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

Credit is given to Kyle Burns of PacketLabs 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	R6.4.0.HF1 (R6.4.0.136) and earlier	R6.4.0.HF2 (R6.4.0.137) or later
Mitel 6900 Series SIP Phones	R6.4.0.HF1 (R6.4.0.136) and earlier	R6.4.0.HF2 (R6.4.0.137) or later
Mitel 6900 Series SIP Phones	R6.4.0.HF1 (R6.4.0.136) and earlier	R6.4.0.HF2 (R6.4.0.137) or later
Mitel 6970 Conference Unit	R6.4.0.HF1 (R6.4.0.136) and earlier	R6.4.0.HF2 (R6.4.0.137) or later

RISK / EXPOSURE

Command Injection in the Boot Process (CVE-2024-41710)

A command injection vulnerability in the 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit, could allow an authenticated attacker with administrative privilege to conduct a command injection attack due to insufficient parameter sanitization during the boot process.

A successful exploit of this vulnerability could allow an attacker to execute arbitrary commands within the context of the phone, with potential impacts on the confidentiality, integrity, and availability of the device.

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

Mitel
Powering connections

	CVSS v3.1
CVSS OVERALL SCORE:	7.2
CVSS VECTOR:	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE:	7.2
CVSS TEMPORAL SCORE:	Not Defined
CVSS ENVIRONMENTAL SCORE:	Not Defined
OVERALL RISK LEVEL:	High

MITIGATION / WORKAROUNDS

There is no specific mitigation for the vulnerability. Customers with affected product versions should upgrade to the highlighted solution versions or later.

SOLUTION INFORMATION

These issues are corrected in Mitel 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit, versions 6.4 HF2 or later. Customers are advised to upgrade to this or a subsequent release.

Please see Mitel Knowledge Base article KB000115993, “Mitel 6800 Series, 6900 Series and 6900w Series SIP Phones, including 6970 Conference Unit Security Update, CVE-2024-41710 and CVE-2024-41711, Command Injection 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	2024-07-17	Initial version
2.0	2024-07-30	Updated the CVE Number

Mitel
Powering connections