

CVE-2024-41710

Mitel SIP Phones Argument Injection Vulnerability

CISA KEV since Feb 12, 2025

Actively exploited

A vulnerability in the Mitel 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit, through R6.4.0.HF1 (R6.4.0.136) could allow an authenticated attacker with administrative privilege to conduct an argument injection attack, due to insufficient parameter sanitization during the boot process. A successful exploit could allow an attacker to execute arbitrary commands within the context of the system.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.2 High · NVD	EPSS 0.416 98.7th percentile · FIRST	CISA DEADLINE Mar 5, 2025 KEV since 2025 · listed over a year
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.416 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions · 22 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
6970 firmware	≤ 6.4.0.136	after 6.4.0.136	NVD
6940w sip firmware	≤ 6.4.0.136	after 6.4.0.136	NVD
6930w sip firmware	≤ 6.4.0.136	after 6.4.0.136	NVD
6920w sip firmware	≤ 6.4.0.136	after 6.4.0.136	NVD
6920 sip firmware	≤ 6.4.0.136	after 6.4.0.136	NVD
6915 sip firmware	≤ 6.4.0.136	after 6.4.0.136	NVD
6910 sip firmware	≤ 6.4.0.136	no fixed version listed	NVD
6905 sip firmware	≤ 6.4.0.136	no fixed version listed	NVD

Sources

Vendor guidance mitel.com/support/security-advisories

mitel.com mitel.com/-/media/mitel/file/pdf/support/security-advisories/security-bulletin_24-0019-001-v2.pdf

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evaluable.com/vulnerability-management/cve/CVE-2024-41710

NVD nvd.nist.gov/vuln/detail/CVE-2024-41710

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-39154

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.