

CVE-2022-41223

Mitel MiVoice Connect Code Injection Vulnerability

CISA KEV since Feb 21, 2023

Actively exploited

Ransomware use known

The Director database component of MiVoice Connect through 19.3 (22.22.6100.0) could allow an authenticated attacker to conduct a code-injection attack via crafted data due to insufficient restrictions on the database data type.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 6.8 Medium · NVD	EPSS 0.107 95.8th percentile · FIRST	CISA DEADLINE Mar 14, 2023 KEV since 2023 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.107 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
mivoice connect	≤ 22.22.6100.0	after 22.22.6100.0	NVD

Sources

Vendor guidance mitel.com/support/security-advisories

mitel.com mitel.com/support/security-advisories/mitel-product-security-advisory-22-0008

NVD nvd.nist.gov/vuln/detail/CVE-2022-41223

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-44464

Current data evulnable.com/vulnerability-management/cve/CVE-2022-41223

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