

CVE-2024-41713

Mitel MiCollab Path Traversal Vulnerability

Exigent

CISA KEV since Jan 7, 2025

Actively exploited

Ransomware use known

A vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab through 9.8 SP1 FP2 (9.8.1.201) could allow an unauthenticated attacker to conduct a path traversal attack, due to insufficient input validation. A successful exploit could allow unauthorized access, enabling the attacker to view, corrupt, or delete users' data and system configurations.

EVRS 93/100 Immediate priority	CVSS V3.1 9.1 Critical · NVD	EPSS 0.972 99.9th percentile · FIRST	CISA DEADLINE Jan 28, 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	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.972 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
micollab	≤ 9.8.1.201	after 9.8.1.201	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-8v9w-9wj4-52p3	Additional guidance	mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029
NVD	nvd.nist.gov/vuln/detail/CVE-2024-41713	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-39339	Current data	evulnabale.com/vulnerability-management/cve/CVE-2024-41713

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