مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in Mitel MiCollab

Tracking #:432316598

Date:06-12-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed researchers have discovered and released a proof-of-concept (PoC) exploit for critical vulnerabilities in Mitel MiCollab, a widely used enterprise collaboration platform.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2024-41713) has been discovered in the Mitel MiCollab system, which affects the NuPoint Unified Messaging (NPM) component. This vulnerability, rated with a CVSS score of 9.8, allows attackers to exploit an insufficient input validation flaw, enabling path traversal attacks. This can give unauthenticated attackers unauthorized access to sensitive information such as system files. This advisory also references CVE-2024-35286, a critical SQL injection vulnerability that could permit attackers to manipulate database operations

Vulnerability Overview

1. CVE-2024-41713 (CVSS 9.8,Critical)

- Affects the NuPoint Unified Messaging (NPM) component
- Allows unauthenticated path traversal attacks
- Enables access to sensitive information and unauthorized administrative actions

2. CVE-2024-35286: SQL Injection Vulnerability

- Severity: Critical (CVSS 9.8, Critical)
- Vulnerability Type: SQL injection flaw affecting NPM.
- Exploit Impact: Attackers could exploit the SQL injection to execute arbitrary database operations and potentially gain unauthorized access to sensitive information or perform unauthorized administrative actions.

Fixed Version:

- MiCollab versions 9.8 SP2 (9.8.2.12) or later

RECOMMENDATIONS:

- All organizations using the affected version should immediately upgrade to the latest patched version of MiCollab to mitigate both vulnerabilities.
- Administrators should audit server and application logs for unusual access patterns or unauthorized attempts to exploit these vulnerabilities.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-00295