April 12, 2024

Overall Rating - High

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Mitel published security advisories to address vulnerabilities in the following product:

- MiCollab – version 9.7.1.110 and prior

Technical Details

A Stored Cross-Site Scripting (XSS) vulnerability has been identified in the web conferencing and the suite applications services components of Mitel MiCollab which, if successfully exploited, could allow a malicious actor to execute arbitrary scripts.
Mitel is recommending customers with affected product versions update to the latest release.

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-30157 CVE-2024-30158 CVE-2024-30159 CVE-2024-30160
- Mitel Security Advisory - 24-0004
- Mitel Security Advisory - 24-0005
- Mitel Security Bulletins