May 23, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

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

- Mitel MiCollab – version 9.7.1.110 and prior, version 9.8.0.33 and prior
- Mitel MiVoice Business Solution Virtual Instance (MiVB SVI) – version 1.0.0.25

Technical Details

A SQL injection vulnerability has been identified in NuPoint Unified Messaging (NPM) component of Mitel MiCollab which, if successfully exploited, could allow a malicious actor to conduct a SQL injection attack.

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

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

References

- CVE-2024-35285 CVE-2024-35286 CVE-2024-35314 CVE-2024-35315
- Mitel security advisory HPE Security Bulletin – 24-0013
- Mitel security advisory HPE Security Bulletin – 24-0014
- Mitel security advisory HPE Security Bulletin – 24-0015
- Mitel security advisory HPE Security Bulletin – 24-0016
- Mitel Security Advisories