July 25, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

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

- Mitel MiCollab – version 9.8 SP1 (9.8.1.5) and prior
- Mitel MiVB – version 1.0.0.27 and prior
- Mitel 6800 Series SIP Phones – version R6.4.0.HF1 (R6.4.0.136) and prior
- Mitel 6900 Series SIP Phones – version R6.4.0.HF1 (R6.4.0.136) and prior
- Mitel 6900w Series SIP Phone – version R6.4.0.HF1 (R6.4.0.136) and prior
- Mitel 6970 Conference Unit – version R6.4.0.HF1 (R6.4.0.136) and prior

Technical Details

A malicious client can send many DNS messages over TCP, potentially causing the server to become unstable while the attack is in progress. The server may recover after the attack ceases. Use of ACLs will not mitigate the attack.

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

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 at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-41712 CVE-2024-35287 CVE-2024-41714
- Mitel security advisory - 24-0022
- Mitel security advisory - 24-0023
- Mitel Security Advisories
-