

Overall rating: Critical



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Mitel published a security advisory to address a vulnerability in the following products:

- Mitel InAttend – versions 2.6 SP4 to 2.7
- Mitel CMG – versions 8.5 SP4 to 8.6

Technical Details

These issues are corrected in Mitel InAttend version 2.8 and Mitel CMG version 8.7. Customers are advised to upgrade to these or subsequent releases. Please see Mitel Knowledge Base article SO7977, “Mitel InAttend and Mitel CMG Security Update, CVE 2024-28815” at https://mitel.custhelp.com/app/answers/answer_view/a_id/1020393, for more information. If you do not have access to this link, please contact your Mitel Authorized Partner for support.

Exploitability Metrics

Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

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-2024-28815
- [Mitel Security Advisory - 24-0003](#)
- [Mitel Security Bulletins](#)