

**Overall rating: Critical**



**This is a technical bulletin intended for technical audiences.**

## Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of Mitel Product Security Advisories. The vulnerability affects MiContact Center Business 10.0.0.4 Hotfix KB560110 and earlier.

## Technical Details

A stored cross-site scripting (XSS) vulnerability has been identified in the Ignite component of Mitel MiContact Center Business which, if successfully exploited, could allow a malicious actor to execute arbitrary scripts. Additionally, a reflected cross-site scripting (XSS) vulnerability has been identified in the Legacy Chat component of Mitel MiContact Center Business which, if successfully exploited, could allow a malicious actor to execute arbitrary scripts.

This vulnerability is rated as a **CRITICAL** 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.

## References

- [Mitel Product Security Advisory 24-0011](#)
- [Mitel Product Security Advisory 24-0012](#)
- [VRM Vulnerability Reports](#)