February 23, 2024

Overall rating: Medium

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability in the Live Data server of Cisco Unified Intelligence Center. The vulnerability affects Cisco Unified Intelligence Center if it had the Live Data server enabled.

Technical Details

A vulnerability in the Live Data server of Cisco Unified Intelligence Center could allow an unauthenticated, local attacker to read and modify data in a repository that belongs to an internal service on an affected device.

This vulnerability is due to insufficient access control implementations on cluster configuration CLI requests. An attacker could exploit this vulnerability by sending a cluster configuration CLI request to specific directories on an affected device. A successful exploit could allow the attacker to read and modify data that is handled by an internal service on the affected device.

Exploitability Metrics
Attack Vector: Local
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **MEDIUM** risk. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

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-2024-20325
- Cisco Unified Intelligence Center Insufficient Access Control Vulnerability
- VRM Vulnerability Reports