

**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 restricted security domain implementation of Cisco Application Policy Infrastructure Controller (APIC). The vulnerability affects Cisco APIC when restricted security domains were configured.

## Technical Details

A vulnerability in the restricted security domain implementation of Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, remote attacker to read, modify, or delete non-tenant policies (for example, access policies) created by users associated with a different security domain on an affected system.

This vulnerability is due to improper access control when restricted security domains are used to implement multi-tenancy for policies outside the tenant boundaries. An attacker with a valid user account associated with a restricted security domain could exploit this vulnerability. A successful exploit could allow the attacker to read, modify, or delete policies created by users associated with a different security domain. Exploitation is not possible for policies under tenants that an attacker has no authorization to access.

### **Exploitability Metrics**

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

This vulnerability is rated as a **MEDIUM** risk. A software patch 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

- [CVE-2023-20230](#)
- [Cisco Application Policy Infrastructure Controller Unauthorized Policy Actions Vulnerability](#)
- [Cisco Security Advisories](#)

***Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.***

You will be able to find all the reports that we have published as well as all future reports here:

<https://bcgov.sharepoint.com/sites/CITZ-ISB/SitePages/vulnerability-reports.aspx>

If you have any questions, please reach out to [OCIOSecurity@gov.bc.ca](mailto:OCIOSecurity@gov.bc.ca)