August 30, 2023

Overall rating: High

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 Intermediate System-to-Intermediate System (IS-IS) protocol of Cisco NX-OS Software for the Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode. This vulnerability affects Cisco products if they are running Cisco NX-OS Software Release 10.3(2) and the IS-IS protocol is enabled on the software.

Technical Details

The impact of this vulnerability may allow an unauthenticated, adjacent attacker to cause the IS-IS process to unexpectedly restart, which could cause an affected device to reload.

This vulnerability is due to insufficient input validation when parsing an ingress IS-IS packet. An attacker could exploit this vulnerability by sending a crafted IS-IS packet to an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition due to the unexpected restart of the IS-IS process, which could cause the affected device to reload.

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

This vulnerability is rated as a **HIGH** 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-2023-20169
- Cisco Nexus 3000 and 9000 Series Switches IS-IS Protocol Denial of Service 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