December 1, 2023

Overall rating: Medium

BRITISH COLUMBIA

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 endpoint software of Cisco Secure Endpoint for Windows. The vulnerability affects Cisco Secure Endpoint Connector for Windows and Cisco Secure Endpoint Private Cloud.

Technical Details

A vulnerability in the endpoint software of Cisco Secure Endpoint for Windows could allow an authenticated, local attacker to evade endpoint protection within a limited time window.

This vulnerability is due to a timing issue that occurs between various software components. An attacker could exploit this vulnerability by persuading a user to put a malicious file into a specific folder and then persuading the user to execute the file within a limited time window. A successful exploit could allow the attacker to cause the endpoint software to fail to quarantine the malicious file or kill its process.

Exploitability Metrics
Attack Vector: Local
Attack Complexity: High
Privileges Required: Low
User Interaction: Required

This vulnerability is rated as a **MEDIUM** 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

- CVE-2023-20084
- Cisco Secure Endpoint for Windows Scanning Evasion Vulnerability
- VRM Vulnerability Reports