August 30, 2023

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 CLI of Cisco FXOS Software. The vulnerability affects Cisco products if they were running a vulnerable release of Cisco FXOS Software:

- Firepower 1000 Series (CSCwd35726, CSCwd05772)
- Firepower 2100 Series (CSCwd35726, CSCwd05772)
- Firepower 4100 Series (CSCwb91812, CSCwd35722)
- Firepower 9300 Security Appliances (CSCwb91812, CSCwd35722)
- Secure Firewall 3100 Series (CSCwd35726, CSCwd05772).

Technical Details

A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to create a file or overwrite any file on the filesystem of an affected device, including system files.

The vulnerability occurs because there is no validation of parameters when a specific CLI command is used. An attacker could exploit this vulnerability by authenticating to an affected device and using the command at the CLI. A successful exploit could allow the attacker to overwrite any file on the disk of the affected device, including system files. The attacker must have valid administrative credentials on the affected device to exploit this vulnerability.

Exploitability Metrics
Attack Vector: Local
Attack Complexity: Low
Privileges Required: High
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-2023-20234
- Cisco FXOS Software Arbitrary File Write 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