May 23, 2024

Overall Rating - High

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Cisco published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- Cisco Firepower Management Center Software – multiple versions

Technical Details

A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system.
This vulnerability exists because the web-based management interface does not adequately validate user input. An attacker could exploit this vulnerability by authenticating the application and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to obtain any data from the database, execute arbitrary commands on the underlying operating system, and elevate privileges to *root*. To exploit this vulnerability, an attacker would need at least Read Only user credentials.

.These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-20360 CVE-2023-20006 CVE-2022-20760
- Cisco Firepower Management Center Software SQL Injection Vulnerability
- Cisco Security Advisories