10 years CERT-EU

Security Advisory 2024-052

Vulnerability in Cisco FMC Software

May 28, 2024 — v1.0

TLP:CLEAR

History:

- *28/05/2024 — v1.0 – Initial publication*

Summary

On May 22, Cisco released an advisory regarding an SQL injection vulnerability affecting its Firepower Management Center (FMC) Software [1]. If exploited, this vulnerability could allow an attacker to obtain any data from the database, execute arbitrary commands on the underlying operating system, and elevate privileges to root.

It is recommended upgrading affected products.

Technical Details

The vulnerability **CVE-2024-20360** [1], with a CVSS score of 8.8, lies in the web-based management interface of Cisco Firepower Management Center (FMC) Software. It exists because the web-based management interface does not adequately validate user input. An attacker could exploit this vulnerability by authenticating to 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 to be able to access the web-based management interface of the affected device, and to have at least Read Only user credentials.

Affected Products

The following versions of Firepower Management Center (FMC) Software are affected:

- 7.3.X
- 7.2.X before 7.2.5.1
- 7.1.X
- 7.0.X before 7.0.6.1

Cisco provides a tool to check if you version is vulnerable [2].

Recommendations

CERT-EU recommends updating to a fixed version of Cisco FMC software.

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sqli-WFFDnNOs

[2] https://sec.cloudapps.cisco.com/security/center/softwarechecker.x