Cisco Secure Firewall Management Center Software Static Credential Vulnerability

Severity Level: MEDIUM

Components Affected

- From Cisco Secure Firewall Management Center (FMC) from Version 7.0.0 to 10.0.1.

Overview

Cisco Secure Firewall Management Center (FMC) Software contains a hardcoded, static credential for a low-privileged built-in account. A remote attacker with no authentication can use this account to log in to an affected FMC and access sensitive data.

Description

A vulnerability has been identified in the web interface of Cisco Secure Firewall Management Center (FMC) Software that could allow an unauthenticated, remote attacker to gain unauthorized access to an affected device. The issue stems from the presence of static, hardcoded user credentials tied to a low-privileged built-in account within the FMC software. Because these credentials are embedded in the software itself rather than being unique per deployment, any attacker aware of them can use this account to authenticate to the web interface without needing valid credentials of their own. CWE-259: Use of Hard-coded Password.
By exploiting this vulnerability, an attacker can successfully log in to the affected system using the low-privileged account and access sensitive data that is available to that account. While the access gained is limited to what the low-privileged account can view, this still exposes information that should otherwise require authentication to reach.

Although the CVSS scoring for this vulnerability would typically correspond to a Medium severity rating, Cisco has assigned it a Security Impact Rating (SIR) of High. This elevated rating reflects the fact that access gained through this low-privileged account can potentially be combined with other, separate vulnerabilities in Cisco Secure FMC Software to escalate privileges further, potentially leading to a more severe compromise of the affected system beyond what this vulnerability alone would allow.

Cisco has confirmed that this vulnerability is being actively exploited in the wild, and it has been added to CISA's Known Exploited Vulnerabilities (KEV) catalog, underscoring the urgency for organizations running affected FMC deployments to remediate promptly.

CWE-259: Use of Hard-coded Password.
CVSS Base Score: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Cisco Security Impact Rating (SIR): High

Impact

- Information Disclosure
- Elevation of Privilege (when chained with other FMC vulnerabilities)

Solution/ Workarounds

Before installation of the software, please visit the vendor website for more details.

Cisco strongly recommends upgrading to a fixed release or applying the following fixes:

- FMC 7.0 - Cisco_Firepower_Mgmt_Center_Hotfix_GB-7.0.9.1-3.sh.REL.tar
- FMC 7.2 - Cisco_Secure_FW_Mgmt_Center_Hotfix_HL-7.2.11.1-4.sh.REL.tar
- FMC 7.4 - Cisco_Secure_FW_Mgmt_Center_Hotfix_HG-7.4.7.1-3.sh.REL.tar
- FMC 7.6 - Cisco_Secure_FW_Mgmt_Center_Hotfix_CY-7.6.5.1-2.sh.REL.tar
- FMC 7.7 - Cisco_Secure_FW_Mgmt_Center_Hotfix_AM-7.7.12.1-2.sh.REL.tar
- FMC 10.0 - Cisco_Secure_FW_Mgmt_Center_Hotfix_P-10.0.1.1-2.sh.REL.tar

Reference

- https://www.cve.org/CVERecord?id=CVE-2026-20316
- https://cwe.mitre.org/data/definitions/259.html
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.