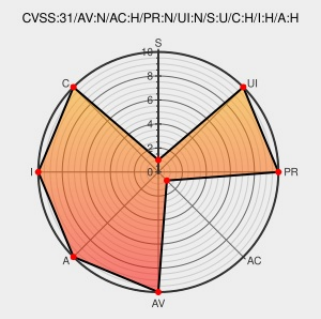
CVE-2020-3410

Published on: 10/21/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:39 PM UTC

CVE-2020-3410 - advisory for cisco-sa-fmc-cacauthbyp-NCLGZm3Q

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Firepower Management Center from Cisco contain the following vulnerability:

A vulnerability in the Common Access Card (CAC) authentication feature of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass authentication and access the FMC system. The attacker must have a valid CAC to initiate the access attempt. The vulnerability is due to incorrect session invalidation during CAC authentication. An attacker could exploit this vulnerability by performing a CAC-based authentication attempt to an affected system. A successful exploit could allow the attacker to access an affected system with the privileges of a CAC-authenticated user who is currently logged in.

CVE-2020-3410 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco Firepower Management Center** version **n/a**

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Cisco Firepower Management Center Software Common Access Card Authentication Bypass Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201021 Cisco Firepower Management Center Software Common Access Card Authentication Bypass Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Firepower Management Center	6.6.0	All	All	All
Application	Cisco	Firepower Management Center	6.6.0.1	All	All	All
Application	Cisco	Firepower Management Center	6.6.0	All	All	All
Application	Cisco	Firepower Management Center	6.6.0.1	All	All	All

cpe:2.3:a:cisco:firepower_management_center:6.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:firepower_management_center:6.6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:firepower_management_center:6.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:firepower_management_center:6.6.0.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→