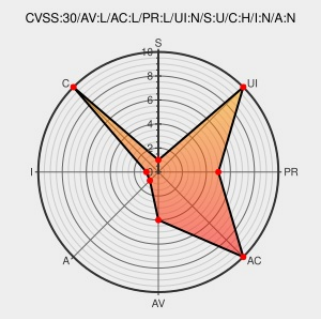
CVE-2021-1126

Published on: 01/13/2021 12:00:00 AM UTC

Last Modified on: 08/05/2022 07:28:00 PM UTC

CVE-2021-1126 - advisory for cisco-sa-fmc-infodisc-RJdktM6f

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



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

A vulnerability in the storage of proxy server credentials of Cisco Firepower Management Center (FMC) could allow an authenticated, local attacker to view credentials for a configured proxy server. The vulnerability is due to clear-text storage and weak permissions of related configuration files. An attacker could exploit this vulnerability by accessing the CLI of the affected software and viewing the contents of the affected files. A successful exploit could allow the attacker to view the credentials that are used to access the proxy server.

CVE-2021-1126 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM 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: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL NONE NONE

CVE References

Description	Tags	Link
Cisco Firepower Management Center Information Disclosure Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20210113 Cisco Firepower Management Center Information Disclosure Vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	All	All	All	All
Application	Cisco	Firepower Management Center	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ? | A vulnerability in the storage of proxy ... | CVE-2021-1126 | Link for more: alerts.remotelyrmm.com/CVE-2021-1126	2022-08-05 21:34:46

← Previous ID Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report