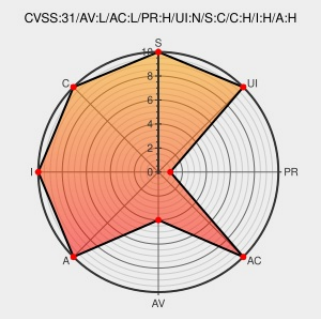
CVE-2021-23882

Published on: 02/10/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:54 PM UTC

CVE-2021-23882

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



Certain versions of Endpoint Security from Mcafee contain the following vulnerability:

Improper Access Control vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update allows local administrators to prevent the installation of some ENS files by placing carefully crafted files where ENS will be installed. This is only applicable to clean installations of ENS as the Access Control rules will prevent modification prior to up an upgrade.

CVE-2021-23882 has been assigned by psirt@mcafee.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **McAfee LLC** - **Endpoint Security (ENS) for Windows** version **< 10.7.0 February 2021**

CVSS3 Score: 4.4 - MEDIUM

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

CVSS2 Score: 1.9 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link

McAfee Security Bulletin - Endpoint Security for Windows update fixes five vulnerabilities (CVE-2021-23878, CVE-2021-23880, CVE-2021-23881, CVE-2021-23882, CVE-2021-23883)	Vendor Advisory kc.mcafee.com text/html	CONFIRM kc.mcafee.com/corporate/index?page=content&id=SB10345

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcafee	Endpoint Security	All	All	All	All
Application	Mcafee	Endpoint Security	All	All	All	All

cpe:2.3:a:mcafee:endpoint_security:*:*:*:*:*:windows:*:*:

cpe:2.3:a:mcafee:endpoint_security:*:*:*:*:*:windows:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→