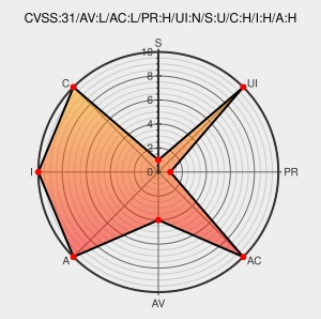
CVE-2021-23879

Published on: 03/15/2021 12:00:00 AM UTC

Last Modified on: 05/03/2022 01:04:00 PM UTC

CVE-2021-23879

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



Certain versions of Endpoint Product Removal Tool from Mcafee contain the following vulnerability:

Unquoted service path vulnerability in McAfee Endpoint Product Removal (EPR) Tool prior to 21.2 allows local administrators to execute arbitrary code, with higher-level privileges, via execution from a compromised folder. The tool did not enforce and protect the execution path. Local admin privileges are required to place the files in the required location.

CVE-2021-23879 has been assigned by psirt@mcafee.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **McAfee, LLC** - **Endpoint Product Removal Tool** version **< 21.2**

CVSS3 Score: 6.7 - MEDIUM

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

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link

McAfee Security Bulletin - Endpoint Product Removal Tool update fixes a Privilege escalation vulnerability (CVE-2021-23879)	Vendor Advisory kc.mcafee.com text/html	CONFIRM kc.mcafee.com/corporate/index?page=content&id=SB10351

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 Product Removal Tool	All	All	All	All

cpe:2.3:a:mcafee:endpoint_product_removal_tool:*:*:*:*:*:*:*:*:

Discovery Credit

McAfee credits Lockheed Martin Red Team for responsibly reporting this flaw.

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ??? | Unquoted service path vulnerability in M... | CVE-2021-23879 | Link for more: alerts.remotelyrmm.com/CVE-2021-23879	2022-04-27 10:28:46

← Previous ID

Next ID→