



CVE-2020-7264

Published on: 05/08/2020 12:00:00 AM UTC

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

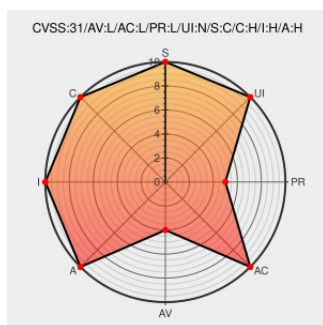
CVE-2020-7264

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Endpoint Security](#) from [Mcafee](#) contain the following vulnerability:

Privilege Escalation vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 Hotfix 199847 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the

target machine.

CVE-2020-7264 has been assigned by psirt@mcafee.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **McAfee,LLC - McAfee Endpoint Security (ENS) for Windows** version < **10.7.0 Hotfix 199847**

CVSS3 Score: **8.4 - HIGH**

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

CVSS2 Score: **3.6 - LOW**

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

CVE References

Description	Tags	Link
-------------	------	------

McAfee Security Bulletin - Endpoint products update to protect against arbitrary file deletion via symbolic links vulnerability (CVE-2020-7264, CVE-2020-7265, CVE-2020-7266, CVE-2020-7267)

Vendor Advisory
kc.mcafee.com
text/html

CONFIRM
kc.mcafee.com/corporate/index?page=content&id=SB10316

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	Mcafee	Endpoint Security	All	All	All	All
Application	Mcafee	Endpoint Security	10.6.0	All	All	All
Application	Mcafee	Endpoint Security	10.7.0	All	All	All
Application	Mcafee	Endpoint Security	All	All	All	All
Application	Mcafee	Endpoint Security	10.6.0	All	All	All
Application	Mcafee	Endpoint Security	10.7.0	All	All	All
cpe:2.3:a:mcafee:endpoint_security:*:*:*:*:windows:*:*:						
cpe:2.3:a:mcafee:endpoint_security:10.6.0:*:*:*:*:windows:*:*:						
cpe:2.3:a:mcafee:endpoint_security:10.7.0:*:*:*:*:windows:*:*:						
cpe:2.3:a:mcafee:endpoint_security:*:*:*:*:*:windows:*:*:						
cpe:2.3:a:mcafee:endpoint_security:10.6.0:*:*:*:*:windows:*:*:						
cpe:2.3:a:mcafee:endpoint_security:10.7.0:*:*:*:*:windows:*:*:						

Discovery Credit

Rack911 Labs discovered this vulnerability.

[← 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 registered 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](#)