

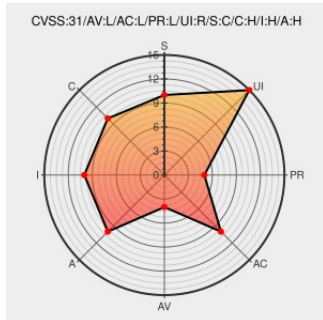


CVE-2020-7250

Published on: 04/15/2020 12:00:00 AM UTC

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

CVE-2020-7250

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Symbolic link manipulation vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2020 Update allows authenticated local user to potentially gain an escalation of privileges by pointing the link to files which the user which not normally have permission to alter via carefully creating symbolic links from the ENS log file directory.

CVE-2020-7250 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) version < 10.7.0 April 2020 Update**

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

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

CVE References

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

McAfee Security Bulletin - Endpoint Security for Windows update fixes multiple vulnerabilities (CVE-2020-7250, CVE-2020-7255, CVE-2020-7257, CVE-2020-7259, CVE-2020-7261, CVE-2020-7273, CVE-2020-7274, CVE-2020-7275, CVE-2020-7276, CVE-2020-7277, CVE-2020-7278)

Vendor Advisory

kc.mcafee.com

text/html

 CONFIRM

kc.mcafee.com/corporate/index?page=content&id=SB10309

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	10.5.0	All	All	All
Application	Mcafee	Endpoint Security	10.5.1	All	All	All
Application	Mcafee	Endpoint Security	10.5.2	All	All	All
Application	Mcafee	Endpoint Security	10.5.3	All	All	All
Application	Mcafee	Endpoint Security	10.5.4	All	All	All
Application	Mcafee	Endpoint Security	10.5.5	All	All	All
Application	Mcafee	Endpoint Security	10.6.0	All	All	All
Application	Mcafee	Endpoint Security	10.5.0	All	All	All
Application	Mcafee	Endpoint Security	10.5.1	All	All	All
Application	Mcafee	Endpoint Security	10.5.2	All	All	All
Application	Mcafee	Endpoint Security	10.5.3	All	All	All
Application	Mcafee	Endpoint Security	10.5.4	All	All	All
Application	Mcafee	Endpoint Security	10.5.5	All	All	All
Application	Mcafee	Endpoint Security	10.6.0	All	All	All

cpe:2.3:a:mcafee:endpoint_security:10.5.0:*:*:*:windows:*:*:

cpe:2.3:a:mcafee:endpoint_security:10.5.1:*:*:*:windows:*:*:

cpe:2.3:a:mcafee:endpoint_security:10.5.2:*:*:*:windows:*:*:

cpe:2.3:a:mcafee:endpoint_security:10.5.3:*:*:*:windows:*:*:

cpe:2.3:a:mcafee:endpoint_security:10.5.4:*:*:*:windows:*:*:

cpe:2.3:a:mcafee:endpoint_security:10.5.5:*:*:*:windows:*:*:

cpe:2.3:a:mcafee:endpoint_security:10.6.0:*:*:*:windows:*:*:

cpe:2.3:a:mcafee:endpoint_security:10.5.0:*:*:*:windows:*:*:

cpe:2.3:a:mcafee:endpoint_security:10.5.1:*:*:*:windows:*:*:

cpe:2.3:a:mcafee:endpoint_security:10.5.2:*:*:*:windows:*:*:
cpe:2.3:a:mcafee:endpoint_security:10.5.3:*:*:*:windows:*:*:
cpe:2.3:a:mcafee:endpoint_security:10.5.4:*:*:*:windows:*:*:
cpe:2.3:a:mcafee:endpoint_security:10.5.5:*:*:*:windows:*:*:
cpe:2.3:a:mcafee:endpoint_security:10.6.0:*:*:*:windows:*:*:

Discovery Credit

McAfee credits Jakub Palaczynski (ING Tech Poland) and Eran Shimony (CyberArk) for independently reporting this flaw