



CVE-2020-7284

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-7284
State	PUBLIC
Assigner	psirt@mcafee.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-03 19:15:00 UTC
Updated	2023-11-07 03:25:00 UTC
Description	Exposure of Sensitive Information in McAfee Network Security Management (NSM) prior to 10.1.7.7 allows local users to g

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcafee	Network Security Management	All	All	All	All
Application	Mcafee	Network Security Management	All	All	All	All

References

Reference	Source
McAfee Security Bulletin - Network Security Manager update fixes Exposure of Sensitive Information vulnerability (CVE-2020-7284)	
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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