



CVE-2020-7258

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

Summary

CVE	CVE-2020-7258
State	PUBLIC
Assigner	psirt@mcafee.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-18 21:15:00 UTC
Updated	2023-11-07 03:25:00 UTC
Description	Cross site scripting vulnerability in McAfee Network Security Management (NSM) Prior to 9.1 update 6 Mar 2020 Update all

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
McAfee Security Bulletin - Network Security Manager/Network Security Platform/Network Threat Behavior Analysis update fixes multiple vulne
CVE Program record
NVD vulnerability detail

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