



CVE-2022-0166

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

Summary

CVE	CVE-2022-0166
State	PUBLIC
Assigner	psirt@mcafee.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-19 11:15:00 UTC
Updated	2023-11-07 03:41:00 UTC
Description	A privilege escalation vulnerability in the McAfee Agent prior to 5.7.5. McAfee Agent uses openssl.cnf during the build process.

Risk And Classification

Problem Types: CWE-427

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcafee	Agent	All	All	All	All

References

Reference	Source	Link
VU#287178 - McAfee Agent for Windows is vulnerable to privilege escalation due to OPENSSLDIR location		www.kb.cert.org
Security Bulletin - McAfee Agent update fixes two vulnerabilities (CVE-2021-31854, CVE-2022-0166)		kc.mcafee.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[376433](#) McAfee Agent Multiple Vulnerabilities (SB10378)

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](#)