



CVE-2016-2208

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2016-2208
State	PUBLIC
Assigner	secure@symantec.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-19 10:59:00 UTC
Updated	2016-12-01 03:08:00 UTC
Description	The kernel component in Symantec Anti-Virus Engine (AVE) 20151.1 before 20151.1.1.4 allows remote attackers to execut

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Anti-virus Engine	All	All	All	All

References

Reference

- Symantec/Norton AntiVirus - ASPack Remote Heap/Pool Memory Corruption - Multiple dos Exploit
- Symantec Anti Virus Engine Heap Overflow in Processing Files Lets Remote Users Execute Arbitrary Code - SecurityTracker
- 820 - Symantec/Norton Antivirus ASPack Remote Heap/Pool memory corruption Vulnerability CVE-2016-2208 - project-zero - Monorail
- Security Advisories Relating to Symantec Products - Symantec Antivirus Engine Malformed PE Header Parser Memory Access Violation - 20190653
- 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.report](#) 2026 |

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](#)