



CVE-2005-2758

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

Summary

CVE	CVE-2005-2758
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-10-05 19:02:00 UTC
Updated	2017-07-11 01:32:00 UTC
Description	Integer signedness error in the administrative interface for Symantec AntiVirus Scan Engine 4.0 and 4.3 allows remote attac

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Antivirus Scan Engine	4.0	All	All	All
Application	Symantec	Antivirus Scan Engine	4.0	All	bluecoat	All
Application	Symantec	Antivirus Scan Engine	4.0	All	clearswift	All
Application	Symantec	Antivirus Scan Engine	4.0	All	netapp_filer	All
Application	Symantec	Antivirus Scan Engine	4.0	All	netapp_netcache	All
Application	Symantec	Antivirus Scan Engine	4.3	All	All	All
Application	Symantec	Antivirus Scan Engine	4.3	All	clearswift	All
Application	Symantec	Antivirus Scan Engine	4.3	All	clearswift	All
Application	Symantec	Antivirus Scan Engine	4.3	All	microsoft_sharepoint	All
Application	Symantec	Antivirus Scan Engine	4.0	All	All	All
Application	Symantec	Antivirus Scan Engine	4.0	All	bluecoat	All
Application	Symantec	Antivirus Scan Engine	4.0	All	clearswift	All
Application	Symantec	Antivirus Scan Engine	4.0	All	netapp_filer	All
Application	Symantec	Antivirus Scan Engine	4.0	All	netapp_netcache	All
Application	Symantec	Antivirus Scan Engine	4.3	All	All	All
Application	Symantec	Antivirus Scan Engine	4.3	All	clearswift	All
Application	Symantec	Antivirus Scan Engine	4.3	All	clearswift	All

Application	Symantec	Antivirus Scan Engine	4.3	All	microsoft_sharepoint	All
Application	Symantec	Antivirus Scan Engine For Network Attached Storage	4.3	All	All	All
Application	Symantec	Antivirus Scan Engine For Network Attached Storage	4.3	All	All	All

References

Reference

[Symantec AntiVirus Scan Engine Web Service Administrative Interface Buffer Overflow Vulnerability](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[US-CERT Vulnerability Note VU#849209](#)

[Secunia - Advisories - Symantec AntiVirus Scan Engine Administrative Interface Buffer Overflow](#)

[SecurityReason - Symantec AntiVirus Scan Engine Web Service Buffer Overflow Vulnerability](#)

[19854](#)

[IBM X-Force Exchange](#)

[SecurityTracker.com Archives - Symantec Anti Virus Scan Engine Buffer Overflow in Web Service Lets Remote Users Execute Arbitrary Code](#)

[Accenture | Let there be change](#)

[404 Not Found](#)

[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](#)