



CVE-2007-1252

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

Summary

CVE	CVE-2007-1252
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-03-03 20:19:00 UTC
Updated	2017-07-29 01:30:00 UTC
Description	Buffer overflow in Symantec Mail Security for SMTP 5.0 before Patch 175 allows remote attackers to cause a denial of serv

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Mail Security	5.0	All	smtp	All
Application	Symantec	Mail Security	5.0	All	smtp	All

References

Reference	Source
IBM X-Force Exchange	XF
33840	OSVDB
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
ftp.symantec.com/public/english_us_canada/products/symantec_mail_security/5.0_...	MISC
Symantec Mail Security for SMTP Arbitrary Code Execution Vulnerability	BID
Symantec Mail Security for SMTP Message Handling Vulnerabilities - Advisories - Secunia	SECUNIA
US-CERT Vulnerability Note VU#875633	CERT-VN
Symantec Mail Security for SMTP Message Processing Bug May Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK
CVE Program record	CVE.ORG
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.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](#)