



CVE-2005-2996

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

Summary

CVE	CVE-2005-2996
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-09-20 22:03:00 UTC
Updated	2008-09-05 20:53:00 UTC
Description	Multiple heap-based and stack-based buffer overflows in certain DCOM server components in VERITAS Storage Exec Stor

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec Veritas	Storagecentral	5.2_rev._2190r	All	All	All
Application	Symantec Veritas	Storagecentral	5.2_rev._2190r	All	All	All
Application	Symantec Veritas	Storage Exec	5.3_rev._2190r	All	All	All
Application	Symantec Veritas	Storage Exec	5.3_rev._2190r	All	All	All

References

Reference	Source	Link
US-CERT Vulnerability Note VU#927793	CERT-VN	www.kb.cert.org
US-CERT Vulnerability Note VU#620497	CERT-VN	www.kb.cert.org
Symantec Security Center	CONFIRM	securityresponse.symantec.com
Secunia - Advisories - VERITAS Storage Exec / StorageCentral DCOM Server Buffer Overflow	SECUNIA	secunia.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.

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](#)