



CVE-2006-0989

Published on: 03/27/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:06 PM UTC

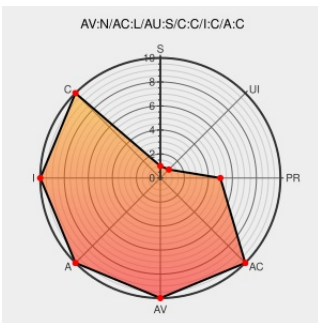
CVE-2006-0989

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of **Netbackup** from **Veritas** contain the following vulnerability:

Stack-based buffer overflow in the volume manager daemon (vmd) in Veritas NetBackup Enterprise Server 5.0 through 6.0 and DataCenter and BusinessServer 4.5FP and 4.5MP allows attackers to execute arbitrary code via unknown vectors.

CVE-2006-0989 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **9 - HIGH**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

SINGLE

Confidentiality Impact

Integrity Impact

Availability Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

Symantec Security Advisory SYM06-006: Multiple overflow vulnerabilities exist in Veritas NetBackup (tm) daemons that could potentially lead to execution of arbitrary code resulting in possible unauthorized, elevated privileged access to the targeted system.

[Vendor Advisory](#)
[seer.support.veritas.com](#)
[text/html](#)

[CONFIRM](#) [seer.support.veritas.com/docs/281521.htm](#)

US-CERT Vulnerability Note VU#880801

[US Government Resource](#)
[www.kb.cert.org](#)
[text/html](#)

[CERT-VN VU#880801](#)

VERITAS NetBackup Multiple Remote Buffer Overflow

[cve.report \(archive\)](#)
[text/html](#)

[BID 17264](#)

Remote Buffer Overflow Vulnerabilities	text/html	
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060327 ZDI-06-005: Symantec VERITAS NetBackup Volume Manager Buffer Overflow
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF netbackup-vmd-sscanf-bo(25471)
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24172
Veritas NetBackup: Multiple Overflow Vulnerabilities in NetBackup Daemons	securityresponse.symantec.com text/html	CONFIRM securityresponse.symantec.com/avcenter/security/Content/2006.03.27.html
SecurityReason	securityreason.com text/html	SREASON 639
ZDI-06-005 Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-06-005.html
SecurityTracker.com Archives - Veritas NetBackup Buffer Overflows in vmd, bpdbm, and bpspsserver Daemons Let Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRAK 1015832
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-1124

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Veritas	Netbackup	4.5.0	fp	businessserver	All
Application	Veritas	Netbackup	4.5.0	fp	datacenter	All
Application	Veritas	Netbackup	4.5.0	mp	businessserver	All
Application	Veritas	Netbackup	4.5.0	mp	datacenter	All
Application	Veritas	Netbackup	5.0	All	enterprise_server	All
Application	Veritas	Netbackup	5.0	All	server	All
Application	Veritas	Netbackup	5.1	All	enterprise_server	All
Application	Veritas	Netbackup	5.1	All	server	All
Application	Veritas	Netbackup	6.0	All	enterprise_server	All
Application	Veritas	Netbackup	6.0	All	server	All

Application	Veritas	Netbackup	4.5.0	tp	businessserver	All
Application	Veritas	Netbackup	4.5.0	fp	datacenter	All
Application	Veritas	Netbackup	4.5.0	mp	businessserver	All
Application	Veritas	Netbackup	4.5.0	mp	datacenter	All
Application	Veritas	Netbackup	5.0	All	enterprise_server	All
Application	Veritas	Netbackup	5.0	All	server	All
Application	Veritas	Netbackup	5.1	All	enterprise_server	All
Application	Veritas	Netbackup	5.1	All	server	All
Application	Veritas	Netbackup	6.0	All	enterprise_server	All
Application	Veritas	Netbackup	6.0	All	server	All
cpe:2.3:a:veritas:netbackup:4.5.0:fp:businessserver:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:4.5.0:fp:datacenter:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:4.5.0:mp:businessserver:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:4.5.0:mp:datacenter:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:5.0:*:enterprise_server:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:5.0:*:server:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:5.1:*:enterprise_server:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:5.1:*:server:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:6.0:*:enterprise_server:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:6.0:*:server:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:4.5.0:fp:businessserver:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:4.5.0:fp:datacenter:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:4.5.0:mp:businessserver:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:4.5.0:mp:datacenter:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:5.0:*:enterprise_server:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:5.0:*:server:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:5.1:*:enterprise_server:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:5.1:*:server:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:6.0:*:enterprise_server:*:*:*:*:						
cpe:2.3:a:veritas:netbackup:6.0:*:server:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#)