



# CVE-2005-3116

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

## Summary

<b>CVE</b>	CVE-2005-3116
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-11-18 06:03:00 UTC
<b>Updated</b>	2017-07-11 01:33:00 UTC
<b>Description</b>	Stack-based buffer overflow in a shared library as used by the Volume Manager daemon (vmd) in VERITAS NetBackup En

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.0_with_mp1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.0_with_mp2	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.0_with_mp3	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.0_with_mp4	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.0_with_mp5	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.1_without_mp	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.1_with_mp1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.1_with_mp2	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.1_with_mp3a	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.0_with_mp1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.0_with_mp2	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.0_with_mp3	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.0_with_mp4	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.0_with_mp5	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.1_without_mp	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.1_with_mp1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.1_with_mp2	All	All	All

Application	<a href="#">Symantec Veritas</a>	<a href="#">Netbackup</a>	5.1_with_mp3a	All	All	All
-------------	----------------------------------	---------------------------	---------------	-----	-----	-----

## References

Reference
<a href="#">SecurityTracker.com Archives - Veritas NetBackup Buffer Overflow in vmd Shared Library Lets Remote Users Execute Arbitrary Code</a>
<a href="#">SecurityFocus</a>
<a href="#">SecurityFocus</a>
<a href="#">Symantec Advisory SYM05-024: Exploitation of a buffer overflow vulnerability in VERITAS NetBackup (tm) Enterprise Server/Server 5.0 and 5</a>
<a href="#">Webmail : Solution de messagerie professionnelle - OVHcloud- OVH</a>
<a href="#">VERITAS NetBackup Volume Manager Daemon Buffer Overflow Vulnerability</a>
<a href="#">Advisory: 11.10.05 // VeriSign iDefense</a>
<a href="#">20674</a>
<a href="#">IBM X-Force Exchange</a>
<a href="#">Secunia - Advisories - VERITAS NetBackup "vmd" Shared Library Buffer Overflow Vulnerability</a>
<a href="#">US-CERT Vulnerability Note VU#574662</a>
<a href="#">VERITAS NetBackup 5.x: Buffer Overflow in Shared Library used by Volume Manager Daemon</a>
<a href="#">CVE Program record</a>
<a href="#">NVD vulnerability detail</a>

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](#)**