

# [NEWS] Symantec VERITAS Multiple Buffer Overflows

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00089.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 29 Mar 2006 16:20:31 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Symantec VERITAS Multiple Buffer Overflows

---

## SUMMARY

<<http://www.veritas.com/>> Symantec VERITAS NetBackup is a backup server and backup client.

Improper bound checking allows attackers to execute arbitrary code in Symantec VERITAS.

## DETAILS

Vulnerable Systems:

- \* VERITAS NetBackup 6.0 Client
- \* VERITAS NetBackup 6.0 Server

vnetd Buffer Overflow:

This specific flaw exists within specially crafted messages to the vnetd service, listening on TCP port 13724 via opcode 6 (Request Service). An attacker can overrun two fixed size buffers, one on the stack, and the other in the .data section of the executable.

In the main function of bpspsserver, a call to `get_adaptable_string()` at

## [NEWS] Symantec VERITAS Multiple Buffer Overflows

0x0040243A reads in a variable length string from the network in the form of '[len][string]'. This string is then copied via a sprintf() at 0x00402458, and a swprintf() at 0x00402479 into two different fixed sized buffers. The first buffer is on the stack and the second buffer is a global variable.

### Volume Manager Buffer Overflow:

This specific flaw exists within the volume manager daemon (vmd.exe) due to incorrect bounds checking during a call to sscanf() that copies user-supplied data to a stack-based buffer. The vulnerable daemon listens on TCP port 13701.

### Database Manager Buffer Overflow:

The specific flaw exists within the NetBackup Database Manager service (bpdbm.exe) due to insufficient bounds checking during a call to sprintf() that copies user-supplied data to a stack-based buffer. The vulnerable daemon listens on TCP port 13721.

### Vendor Response:

"Symantec engineers have addressed these issues in all currently supported versions of NetBackup. Symantec engineers did additional reviews and will continue on-going reviews of related file functionality to further enhance the overall security of Veritas NetBackup products and to eliminate any additional potential concerns.

Security updates are available for all supported products. Symantec strongly recommends all customers immediately apply the latest cumulative Security Pack updates or Maintenance Pack releases as indicated for their supported product versions to protect against threats of this nature."

The security update can be found at:

<<http://support.veritas.com/docs/281521>>

<http://support.veritas.com/docs/281521>

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0989>>

CVE-2006-0989

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0990>>

CVE-2006-0990

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0991>>

CVE-2006-0991

### Disclosure Timeline:

2005.12.19 – Digital Vaccine released to TippingPoint customers regarding Database Manager Buffer Overflow

2005.12.20 – Vulnerability reported to vendor regarding Database Manager Buffer Overflow

2006.01.23 – Vulnerability reported to vendor regarding regarding vneta Buffer Overflow

2006.01.23 – Digital Vaccine released to TippingPoint customers regarding vneta Buffer Overflow

[NEWS] Symantec VERITAS Multiple Buffer Overflows

2006.01.23 – Digital Vaccine released to TippingPoint customers regarding Volume Manager Buffer Overflow

2006.01.24 – Vulnerability reported to vendor regarding Volume Manager Buffer Overflow

2006.03.27 – Coordinated public release of advisory

ADDITIONAL INFORMATION

The information has been provided by <<mailto:zdi-disclosures@xxxxxxxx>> zdi-disclosures.

The original article can be found at:

<<http://www.tippingpoint.com/security/advisories/TSRT-06-01.html>>

<http://www.tippingpoint.com/security/advisories/TSRT-06-01.html>,

<<http://www.zerodayinitiative.com/advisories/ZDI-06-005.html>>

<http://www.zerodayinitiative.com/advisories/ZDI-06-005.html>,

<<http://www.zerodayinitiative.com/advisories/ZDI-06-006.html>>

<http://www.zerodayinitiative.com/advisories/ZDI-06-006.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.