Update: February 13, 2006

Buffer Overflow Vulnerability in a Shared Library Used by the Volume Manager Daemon of JP1/VERITAS NetBackup 5.x

- Affected products

Corrective action	Product name	Platform	Last update
HS06-001-01	JP1/VERITAS NetBackup	Windows, AIX, HP-UX, Solaris, Linux	February 13, 2006

- Problem description

The following advice was released on the Symantec website (formerly the VERITAS website): *"VERITAS NetBackup 5.x: Buffer Overflow in Shared Library used by Volume Manager Daemon"*
Malicious remote users can exploit this vulnerability, disrupt the above backup system, and execute arbitrary code

Revision history

- February 13, 2006: This page is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security @itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.

- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

Software Vulnerability Information
Software Division

HITACHI Inspire the Next

| Home | Software | » Security |

Japanese

Search in the Hitachi site by Google
GO
> Advanced search

Home > Vulnerability Information > Software Vulnerability Information > HS06-001-01

Update: February 13, 2006

HS06-001;
Buffer Overflow Vulnerability in a Shared Library Used by the Volume Manager Daemon of JP1/VERITAS NetBackup 5.x

Solution for JP1/VERITAS NetBackup

A buffer overflow vulnerability was found in a shared library that is used by the JP1/VERITAS NetBackup Volume Manager Daemon (vmd) running on JP1/VERITAS NetBackup 5.x and clients. Malicious attackers can exploit the buffer overflow vulnerability to instigate denial-of-service (DoS) attacks on the backup system or execute arbitrary codes with elevated privileges on the targeted system.

[Influence]

The vulnerability affects the backup servers of JP1/VERITAS NetBackup and any servers on which a client is installed.

[Affected models and versions]

Product name	Model	Version	Platform	Last update
JP1/VERITAS NetBackup 5.1	RT-1V25-L20M20	07-10 to 07-13	Windows, AIX, HP-UX, Solaris, Linux	February 13, 2006
JP1/VERITAS NetBackup 5	RT-1V25-L10M20	07-00 to 07-02		February 13, 2006

(*) JP1/VERITAS NetBackup v3.4 and v4.5 are not affected.

[Corrective action]

Contact your Hitachi support service representative, and take corrective action.

Revision history

- February 13, 2006: Information about buffer overflow vulnerability in a shared library used by the Volume Manager Daemon of JP1/VERITAS NetBackup 5.x is released.

TOP

What's New

Notifications

Alert

Software Vulnerability Information

Links to Security Organizations

Email
soft-security @itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top