HITACHI Home | Information Technology Site | Global Sites of related products JAPAN

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 > HS05-021

Update: November 14, 2005

Vulnerability Regarding the Java Interface Function of JP1/VERITAS NetBackup

- Affected products

Corrective action	Product name	Platform	Last update
HS05-021-01	JP1/VERITAS NetBackup	Windows, AIX, HP-UX, Solaris, Linux	November 14, 2005

- Problem description

The following advice was released on the Symantec website (formerly the VERITAS website): *"A vulnerability has recently been discovered, which affects the bpjava-msvc logon process within VERITAS NetBackup (tm) 4.5, 5.0, 5.1, and 6.0 (including maintenance and feature packs). This vulnerability could potentially allow remote malicious users to execute arbitrary code."*
Malicious remote users can exploit the vulnerability, cause a system crash, and execute arbitrary code in the above product.

Revision history

- November 14, 2005: 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

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 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

HITACHI Home   Information Technology Site   Global Sites of related products   JAPAN

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 > HS05-021-01

Update: November 14, 2005

HS05-021;
Vulnerability Regarding the Java Interface Function of JP1/VERITAS NetBackup

Solution for JP1/VERITAS NetBackup

A format string vulnerability that allows attackers to cause a system crash and execute arbitrary code was found in the Java interface of JP1/VERITAS NetBackup.
Please take the corrective action indicated below.

[Influence]
This vulnerability affects the backup servers of JP1/VERITAS NetBackup and any servers for which its client is installed.

[Affected models and versions]

Product name	Model	Version	Platform	Last update
JP1/VERITAS NetBackup 5.1	RT-1V25-L20M20	07-10 - 07-13	Windows, AIX, HP-UX, Solaris, Linux	November 14, 2005
JP1/VERITAS NetBackup 5	RT-1V25-L10M20	07-00 - 07-02		November 14, 2005
JP1/VERITAS NetBackup v4.5	RT-1V25-HN8536C	06-71 - 06-76-/A		November 14, 2005

(*) JP1/VERITAS NetBackup V3.4 is also affected, but the Hitachi support service does not support V3.4 anymore, therefore a corrective patch for V3.4 is not scheduled. Please upgrade V3.4 to the latest version, and then apply the corrective patches.

[Corrective action]
For the fixed versions, contact your Hitachi support service representative.

Revision history

- November 14, 2005: Information about vulnerability regarding the Java interface function of JP1/VERITAS NetBackup 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