Update: February 8, 2005

Vulnerability in JP1/VERITAS NetBackup JavaGUI

- Affected product

Corrective action	Product name	Platform	Last update
HS05-003-01	JP1/VERITAS NetBackup, VERITAS NetBackup	Windows, AIX, HP-UX, Solaris, Linux	February 8, 2005

- Problem description

On December 23, 2004, Veritas released their TechNote titled *"VERITAS NetBackup (tm) Java GUI is susceptible to an exploit which could allow a normal user to execute commands with root authority. Anyone who administers NetBackup via the Java GUI that does not use the work-around listed below could be potentially affected by this exploit"*.
When one of the conditions below is met, a normal user can exploit this vulnerability to send specially crafted commands to the backup server (either a master server or a media server) and have those commands executed with root authority (Administrator permission for Windows).

- JavaGUI is connected to a backup server (either a master server or a media server)
- Backup & Restore GUI is executing with root authority (Administrator permission for Windows)

Revision history

- February 8, 2005: This page 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

Update: February 8, 2005

HS05-003;
Vulnerability in JP1/VERITAS NetBackup JavaGUI

Solution for JP1/VERITAS NetBackup and VERITAS NetBackup

The following vulnerability was found in JP1/VERITAS NetBackup and VERITAS NetBackup:
When one of the conditions below is met, a normal user can send specially crafted commands to the backup server (either a master server or a media server) and have those commands executed with root authority (Administrator permission for Windows).

- JavaGUI is connected to a backup server (either a master server or a media server)
- Backup & Restore GUI is executing with root authority (Administrator permission for Windows)

Please take the corrective actions indicated in the website of VERITAS. For details, see *Corrective actions* below.

[Influence]
This vulnerability affects the backup servers (either master servers or media servers) and any servers that use NetBackup JavaGUI to connect with backup servers.

[Affected models and versions]
Affected Hitachi products and corresponding VERITAS products are as follows:

Product name	Model	Version	Platform	Product name and Version of Veritas	Last update
JP1/VERITAS NetBackup 5.1	RT-1V25-L20M20	07-00 to 07-02	Windows AIX HP-UX Solaris Linux	VERITAS NetBackup 5.1	February 8, 2005
JP1/VERITAS NetBackup 5	RT-1V25-L10M20	07-10 to 07-11	Windows AIX HP-UX Solaris Linux	VERITAS NetBackup 5	February 8, 2005
			Windows		

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

JP1/VERITAS NetBackup v4.5	RT-1V25-HN8536C	06-71 to 06-76-/A	AIX HP-UX Solaris Linux	VERITAS NetBackup v4.5	February 8, 2005
JP1/VERITAS NetBackup V3.4	RT-1V25-D9011330	06-70	Windows AIX HP-UX Solaris	VERITAS NetBackup V3.4	February 8, 2005
	RT-1V25-D9011340				February 8, 2005
	RT-1V25-D9011350				February 8, 2005
VERITAS NetBackup V3.4	RT-1V25-19011330	01-00	Windows AIX HP-UX Solaris	VERITAS NetBackup V3.4	February 8, 2005
	RT-1V25-19011340				February 8, 2005
	RT-1V25-19011350				February 8, 2005
	RT-1V25-1NDSE000				February 8, 2005

[Corrective actions]
Visit the VERITAS website below and take the corrective actions.
http://seer.support.veritas.com/docs/271727.htm

Revision history

- February 8, 2005: Information about the vulnerability in JP1/VERITAS NetBackup JavaGUI 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 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