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

Update: October 11, 2006

Heap Overflow Vulnerability in RPC Interface of JP1/VERITAS Backup Exec for Windows Servers

- Affected products

Corrective action	Product name	Platform	Last update
HS06-015-01	JP1/VERITAS Backup Exec	Windows	October 11, 2006

- Problem description

The following notice was released on the Symantec website (formerly the VERITAS website): *"Symantec Backup Exec for Windows Server: RPC Interface Heap Overflow, Authorized User Potential Elevation of Privilege"*.
Malicious remote users can exploit this vulnerability and execute arbitrary codes.

Revision history

- October 11, 2006: This page is released.

Page Top

| Term of Use | Privacy Notice | About Hitachi |

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

Update: October 11, 2006

HS06-015;
Heap Overflow Vulnerability in RPC Interface of JP1/VERITAS Backup Exec for Windows Servers

Solution for JP1/VERITAS Backup Exec

Heap overflow vulnerability was found in RPC interface of JP1/VERITAS Backup Exec.

[Impact]

The vulnerability affects the media servers of JP1/VERITAS Backup Exec and any servers on which a Remote Agent is installed.

Symantec Security Response (Document ID: SYM06-014) says:
On the media servers and any servers on which a Remote Agent module works, overflows occur due to improper validation and subsequent handling of user input. Malicious users can exploit this vulnerability, execute arbitrary code, and gain elevated privilege on the targeted system.

[Affected models and versions]

Product name(*1)	Model	Version	Platform	Last update
JP1/VERITAS Backup Exec 10d for Windows Servers	RT-1V25-K4W110	07-60		October 11, 2006
		07-61		October 11, 2006
	RT-1V25-K4WL10	07-60		October 11, 2006
		07-61		October 11, 2006
	RT-1V25-K4WC10	07-60		October 11, 2006
		07-61		October 11, 2006
	RT-1V25-K3W110	07-52		October 11, 2006
		07-51		October 11, 2006
		07-50		October

				11, 2006
JP1/VERITAS Backup Exec 10.0 for Windows Servers	RT-1V25-K3WL10	07-52	Windows	October 11, 2006
		07-51		October 11, 2006
		07-50		October 11, 2006
	RT-1V25-K3WC10	07-52		October 11, 2006
	RT-1V25-K3WA10	07-51		October 11, 2006
	RT-1V25-K3WA20	07-50		October 11, 2006
JP1/VERITAS Backup Exec 9.1 for Windows Servers	RT-1V25-K2W110	07-01		October 11, 2006
		07-00		October 11, 2006
	RT-1V25-K2WL10	07-01		October 11, 2006
		07-00		October 11, 2006
	RT-1V25-K2WC10	07-01		October 11, 2006
		07-00		October 11, 2006
	RT-1V25-K2WC20	07-01		October 11, 2006
		07-00		October 11, 2006

(*1) JP1/VERITAS Backup Exec 9.0 for Windows Servers is no longer supported by the Hitachi support service. Please upgrade to the latest version, or carry out the following workarounds.

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]
Until the fixed modules are applied, please carry out the following workarounds:

- Restrict remote access to trusted and authorized systems only.

Revision history

- October 11, 2006: Information about heap overflow vulnerability in RPC interface of JP1/VERITAS Backup Exec for Windows Servers is released.

---

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