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: November 14, 2005

Vulnerability to Administrator Privileges Being Granted for the System Registry in a JP1/VERITAS Backup Exec System

- Affected products

Corrective action	Product name	Platform	Last update
HS05-022-01	JP1/VERITAS Backup Exec	Windows	November 14, 2005

- Problem description

The following advice was released on the Symantec website (formerly the VERITAS website): *"After applying Hotfix 51 or Service Pack 3 for Backup Exec 9.1 for Windows Servers, the Backup Exec remote registry access vulnerability (VX05-003) reoccurs."*
Malicious remote users can exploit the vulnerability and gain Administrator privileges over the system registry on a system containing VERITAS Backup Exec.

Revision history

- November 14, 2005: This page is released.

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

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: November 14, 2005

HS05-022;
Vulnerability to Administrator Privileges Being Granted for the System Registry in a JP1/VERITAS Backup Exec System

Solution for JP1/VERITAS Backup Exec

A vulnerability that allows malicious attackers to gain Administrator privileges over the system registry was found in JP1/VERITAS Backup Exec.
Please take the corrective action indicated below.

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

[Affected models and versions]

Product name	Model	Version	Last update
JP1/VERITAS Backup Exec 9.1 for Windows Servers	RT-1V25-K2W110	07-01	November 14, 2005
		07-00	November 14, 2005
	RT-1V25-K2WL10	07-01	November 14, 2005
		07-00	November 14, 2005

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

Revision history

- November 14, 2005: Information about vulnerability to Administrator privileges being granted for the system registry in a JP1/VERITAS Backup Exec system is released.

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