

Software Vulnerability Information

Software Division



Update: July 20, 2005

Multiple vulnerabilities of JP1/VERITAS Backup Exec

- Affected products

Corrective action	Product name	Platform	Last update
HS05-014-01	JP1/VERITAS Backup Exec	Windows	July 20, 2005

- Problem description

On July 22, 2005, the advice [Security Advisory for Backup Exec for Windows Servers and Backup Exec for NetWare Servers](#) was released on the VERITAS website.

The following vulnerabilities were found in JP1/VERITAS Backup Exec.

- VX05-001(*1)**
Malicious users can exploit the vulnerability of buffer overflow and cause a system crash or DoS (Denial of Service) on server machines for which Remote Control Agent is installed.
- VX05-002(*1)**
Malicious users can exploit the vulnerability of buffer overflow and execute arbitrary codes on server machines for which Remote Control Agent is installed.
- VX05-003(*1)**
Malicious users can exploit the vulnerability and gain Administrator privileges for the system registry on backup server machines.
- VX05-005(*1)**
Malicious users can exploit the vulnerability of buffer overflow and execute arbitrary codes on backup server machines for which Web Administration Console (BEWAC) is installed.
- VX05-006(*1)**
Malicious users can exploit the vulnerability of remote heap overflow and execute arbitrary codes on backup server machines for which Admin Plus Pack Option is installed.
- VX05-007(*1)**
On server machines for which Remote Control Agent is installed,

- > 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



non-privileged malicious remote users can exploit the vulnerability to gain privileges that are equal to the SYSTEM user by copying the handle that the agent uses.

- (*1) VX05-*** (***) is a three digit serial number) is the VERITAS Software Security Advisory number for the VERITAS company. VX05-004 is currently an unused serial number. VX05-008 does not affect JP1/VERITAS products.

Revision history

- July 20, 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 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](#)

Software Vulnerability Information

Software Division



| [Home](#) | [Software](#) | [» Security](#) |

» [Japanese](#)

Search in the Hitachi site by Google



> [Advanced search](#)

[Home](#) > [Vulnerability Information](#) > [Software Vulnerability Information](#) > [HS05-014-01](#)

> [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](#)



Update: July 20, 2005

HS05-014; Multiple vulnerabilities of JP1/VERITAS Backup Exec

Solution for JP1/VERITAS Backup Exec

The following vulnerabilities were found in JP1/VERITAS Backup Exec.

- VX05-001(*1)
Malicious users can exploit the vulnerability of buffer overflow and cause a system crash or DoS (Denial of Service) on server machines for which Remote Control Agent is installed.
- VX05-002(*1)
Malicious users can exploit the vulnerability of buffer overflow and execute arbitrary codes on server machines for which Remote Control Agent is installed.
- VX05-003(*1)
Malicious users can exploit the vulnerability and gain Administrator privileges for the system registry on backup server machines.
- VX05-005(*1)
Malicious users can exploit the vulnerability of buffer overflow and execute arbitrary codes on backup server machines for which Web Administration Console (BEWAC) is installed.
- VX05-006(*1)
Malicious users can exploit the vulnerability of remote heap overflow and execute arbitrary codes on backup server machines for which Admin Plus Pack Option is installed.
- VX05-007(*1)
On server machines for which Remote Control Agent is installed, non-privileged malicious remote users can exploit the vulnerability to gain privileges that are equal to the SYSTEM user by copying the handle that the agent uses.

(*1) VX05-*** (***) is a three digit serial number) is the VERITAS Software Security Advisory number for the VERITAS company. VX05-004 is currently an unused serial number. VX05-008 does not affect JP1/VERITAS products.

Please take the corrective actions as indicated below.

[Influence]

These vulnerabilities affect the backup servers of JP1/VERITAS Backup Exec and any servers for which Remote Console Agent is installed.

[Affected models and versions]

Product name	Model	Version	Last update
JP1/VERITAS Backup Exec 10.0 for Windows Servers	RT-1V25-K3W110	07-51	July 20, 2005
		07-50	July 20, 2005
	RT-1V25-K3WL10	07-51	July 20, 2005
		07-50	July 20, 2005
	RT-1V25-K3WE20	07-50	July 20, 2005
	RT-1V25-K3WC10	07-50	July 20, 2005
	RT-1V25-K3WA10	07-50	July 20, 2005
	RT-1V25-K3WA20	07-50	July 20, 2005
RT-1V25-K3WA30	07-50	July 20, 2005	
JP1/VERITAS Backup Exec 9.1 for Windows Servers	RT-1V25-K2W110	07-01	July 20, 2005
		07-00	July 20, 2005
	RT-1V25-K2WL10	07-01	July 20, 2005
		07-00	July 20, 2005
	RT-1V25-K2WE20	07-00	July 20, 2005
	RT-1V25-K2WC10	07-00	July 20, 2005
	RT-1V25-K2WC20	07-00	July 20, 2005
	RT-1V25-K2WA10	07-00	July 20, 2005
RT-1V25-K2WA20	07-00	July 20, 2005	
RT-1V25-K2WA30	07-00	July 20, 2005	
RT-1V25-K2WE10	07-00	July 20, 2005	
JP1/VERITAS Backup Exec 9.0 for Windows Servers	RT-1V25-K1W110	06-73, 06-74	July 20, 2005
		06-72	July 20, 2005
	RT-1V25-K1WL10	06-73, 06-74	July 20, 2005
		06-72	July 20, 2005
	RT-1V25-K1WU10	06-73, 06-74	July 20, 2005
		06-72	July 20, 2005
	RT-1V25-K1WU20	06-73, 06-74	July 20, 2005
		06-72	July 20, 2005
	RT-1V25-K1WU30	06-73, 06-74	July 20, 2005
		06-72	July 20, 2005
	RT-1V25-K1WC10	06-72	July 20, 2005
	RT-1V25-K1WC20	06-72	July 20, 2005
	RT-1V25-K1WA10	06-72	July 20, 2005
	RT-1V25-K1WG10	06-72	July 20, 2005
RT-1V25-K1WA20	06-72	July 20, 2005	
RT-1V25-K1WG20	06-72	July 20, 2005	
RT-1V25-K1WA30	06-72	July 20, 2005	
RT-1V25-K1WE20	06-72	July 20, 2005	
RT-1V25-K1WE10	06-72	July 20, 2005	

[Corrective action]

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

Revision history

- July 20, 2005: Information about the multiple vulnerabilities of JP1/VERITAS Backup Exec 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](#)