Update: May 17, 2006

DoS and Format String Vulnerabilities in JP1/VERITAS Backup Exec

- Affected products

Corrective action	Product name	Platform	Last update
HS06-008-01	JP1/VERITAS Backup Exec	Windows	May 17, 2006

- Problem description

The following notices were released on the Symantec website (formerly the VERITAS website): *"Veritas Backup Exec and NBU for NetWare Media Server Options: Application Memory Denial of Service"* and *"Veritas Backup Exec for Windows Servers: Media Server BENGINE Service Job log Format String Overflow"*.
Malicious remote users can exploit these vulnerabilities, cause memory errors, and execute arbitrary codes.

Revision history

- May 17, 2006: 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

- 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: May 17, 2006

HS06-008;
DoS and Format String Vulnerabilities in JP1/VERITAS Backup Exec

Solution for JP1/VERITAS Backup Exec

DoS and format string vulnerabilities were found in JP1/VERITAS Backup Exec.

[Impact]

These vulnerabilities affect the media servers of JP1/VERITAS Backup Exec and any servers on which a remote agent is installed.

- Symantec Security Response ID : SYM06-004
  Invalid format packet data that is sent to a Backup Exec remote agent might cause processing to stop or a DoS attack to occur, resulting in multiple memory errors. To recover the system, restart the Backup Exec Remote Agent service.

- Symantec Security Response ID : SYM06-005
  If the job log is set to run in the "Full Details" mode, a format string vulnerability that causes a DoS attack or that allows arbitrary code to be run might occur.

[Affected models and versions]

Product name	Model	Version	Platform	Last update
JP1/VERITAS Backup Exec 10d for Windows Servers	RT-1V25-K4W110	07-60		May 17, 2006
	RT-1V25-K4WL10	07-60		May 17, 2006
	RT-1V25-K4WC10	07-60		May 17, 2006
JP1/VERITAS Backup Exec 10.0 for	RT-1V25-K3W110	07-52		May 17, 2006
		07-51		May 17, 2006
		07-50		May 17, 2006
	RT-1V25-	07-52		May 17, 2006
				May 17,

Windows Servers	K3WL10	07-51		2006
		07-50		May 17, 2006
	RT-1V25-K3WC10	07-52		May 17, 2006
	RT-1V25-K3WA10	07-51		May 17, 2006
	RT-1V25-K3WA20	07-50		May 17, 2006
JP1/VERITAS Backup Exec 9.1 for Windows Servers	RT-1V25-K2W110	07-01	Windows	May 17, 2006
		07-00		May 17, 2006
	RT-1V25-K2WL10	07-01		May 17, 2006
		07-00		May 17, 2006
	RT-1V25-K2WC10	07-01		May 17, 2006
		07-00		May 17, 2006
	RT-1V25-K2WC20	07-01		May 17, 2006
		07-00		May 17, 2006
JP1/VERITAS Backup Exec 9.0 for Windows Servers (*1)	RT-1V25-K1W110	06-74		May 17, 2006
		06-73		May 17, 2006
		06-72		May 17, 2006
	RT-1V25-K1WL10	06-74		May 17, 2006
		06-73		May 17, 2006
		06-72		May 17, 2006
	RT-1V25-K1WU10	06-74		May 17, 2006
		06-73		May 17, 2006
		06-72		May 17, 2006
	RT-1V25-K1WU20	06-74		May 17, 2006
		06-73		May 17, 2006
		06-72		May 17, 2006
	RT-1V25-K1WU30	06-74		May 17, 2006
		06-73		May 17, 2006
		06-72		May 17,

				2006
	RT-1V25-K1WC10	06-72		May 17, 2006
	RT-1V25-K2WC20	06-72		May 17, 2006

(*1) 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, carry out the following workarounds:

- Workaround for SYM06-004
  Set the filtering rules on the router so that access through TCP port 10000 is not allowed.

- Workaround for SYM06-005
  Do not set the job log to run in the "Full Details" mode. Apply the default setting or another setting.

Revision history

- May 17, 2006: Information about DoS and format string vulnerabilities in JP1/VERITAS Backup Exec is released.

Page Top