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: February 8, 2005

Vulnerability of Buffer Overflow in JP1/VERITAS Backup Exec

- Affected product

Corrective action	Product name	Platform	Last update
HS05-002-01	JP1/VERITAS Backup Exec, VERITAS Backup Exec	Windows	February 8, 2005

- Problem description

On December 17, 2004, Veritas released their TechNote titled *"Remote exploitation of a stack-based buffer overflow vulnerability in Backup Exec 8.6 and 9.x may allow the unauthorized execution of arbitrary code"*.
On backup servers of the above products, malicious remote users can exploit the vulnerability of buffer overflow and execute arbitrary code.

Revision history

- February 8, 2005: This page is released.

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: February 8, 2005

HS05-002;
Vulnerability of Buffer Overflow in JP1/VERITAS Backup Exec

Solution for JP1/VERITAS Backup Exec

The following vulnerability was found in JP1/VERITAS Backup Exec and VERITAS Backup Exec:

- Malicious remote users can exploit the vulnerability of buffer overflow and execute arbitrary code on backup servers.

Please apply the workaround or take the corrective action below.

[Influence]
This vulnerability affects the backup servers of JP1/VERITAS Backup Exec and VERITAS Backup Exec. It does not occur on the servers running remote agent.

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

Product name	Model	Version	Product name and Version of Veritas	Last update
JP1/VERITAS Backup Exec 9.1 for Windows Servers	RT-1V25-K2W110	07-01	VERITAS Backup Exec 9.1 for Windows Servers revision4691 SP1	February 8, 2005
		07-00	VERITAS Backup Exec 9.1 for Windows Servers revision4691	February 8, 2005
	RT-1V25-K2WL10	07-01	VERITAS Backup Exec 9.1 for Windows Servers revision4691 SP1	February 8, 2005
		07-00	VERITAS Backup Exec 9.1 for Windows Servers revision4691	February 8, 2005
	RT-1V25-K1W110	06-73, 06-74	VERITAS Backup Exec 9.0 for Windows Servers revision4454	February 8, 2005
		06-72	VERITAS Backup Exec 9.0 for Windows Servers revision4367	February 8, 2005

JP1/VERITAS Backup Exec 9.0 for Windows Servers	RT-1V25-K1WL10	06-73, 06-74	VERITAS Backup Exec 9.0 for Windows Servers revision4454	February 8, 2005
		06-72	VERITAS Backup Exec 9.0 for Windows Servers revision4367	February 8, 2005
	RT-1V25-K1WU10	06-73, 06-74	VERITAS Backup Exec 9.0 for Windows Servers revision4454	February 8, 2005
		06-72	VERITAS Backup Exec 9.0 for Windows Servers revision4367	February 8, 2005
	RT-1V25-K1WU20	06-73, 06-74	VERITAS Backup Exec 9.0 for Windows Servers revision4454	February 8, 2005
		06-72	VERITAS Backup Exec 9.0 for Windows Servers revision4367	February 8, 2005
	RT-1V25-K1WU30	06-73, 06-74	VERITAS Backup Exec 9.0 for Windows Servers revision4454	February 8, 2005
		06-72	VERITAS Backup Exec 9.0 for Windows Servers revision4367	February 8, 2005
JP1/VERITAS Backup Exec for Windows NT/Windows 2000 V8.6	RT-1V25-ANTAS126	06-70	VERITAS Backup Exec for Windows NT/Windows 2000 V8.6 revision3878	February 8, 2005
	RT-1V25-ANTAS130			February 8, 2005
	RT-1V25-ANTSR104			February 8, 2005
	RT-1V25-ANTSR105			February 8, 2005
	RT-1V25-YNTSR104			February 8, 2005
VERITAS Backup Exec for Windows NT/Windows 2000 V8.6	RT-1V25-3NTSR104	08-60	VERITAS Backup Exec for Windows NT/Windows 2000 V8.6 revision3808 or VERITAS Backup Exec for Windows NT/Windows 2000 V8.6 revision3878 (*1)	February 8, 2005
	RT-1V25-3NTSR105			February 8, 2005
	RT-1V25-3NTSR114			February 8, 2005
	RT-1V25-ZNTSR104			February 8, 2005
	RT-1V25-3NTAS126			February 8, 2005
	RT-1V25-3NTAS130			February 8, 2005
VERITAS Backup Exec for Windows NT/Windows 2000 V8.5	RT-1V25-2NTAS860	08-50	VERITAS Backup Exec for Windows NT/Windows 2000 V8.5	February 8, 2005
	RT-1V25-2NTAS890			February 8, 2005
	RT-1V25-2NTSR720			February 8, 2005

(*1) The revision number of VERITAS is either revision 3878 or 3808. Start the GUI of Backup Exec and check the revision number from `[help]` - `[version]`.

[Workarounds]

Protect your backup servers by the firewall system. Otherwise, IP filtering can be used.

[Corrective actions]
See the VERITAS website below and apply the appropriate patch.
http://seer.support.veritas.com/docs/273419.htm
Note: The revision or Service Pack must be applied to both the backup servers and remote agent servers.

Download
9.1 Service Pack 1: http://seer.support.veritas.com/docs/267180.htm
9.1.4691 Hotfix 40: http://seer.support.veritas.com/docs/273420.htm
9.0 revision 4454: http://seer.support.veritas.com/docs/258718.htm
9.0 Service Pack 1: http://seer.support.veritas.com/docs/267151.htm
9.0.4454 Hotfix 30: http://seer.support.veritas.com/docs/274298.htm
8.6 revision 3878: http://seer.support.veritas.com/docs/241038.htm
8.60.3878 Hotfix 68: http://seer.support.veritas.com/docs/273850.htm

Revision history

- February 8, 2005: Information about the vulnerability of buffer overflow in Backup Exec is released.

Page Top

| Term of Use | Privacy Notice | About Hitachi |