

Software Vulnerability Information

Software Division



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

[» Japanese](#)

Search in the Hitachi site by Google



[» Advanced search](#)

[Home](#) > [Vulnerability Information](#) > [Software Vulnerability Information](#) > [HS06-017](#)

Update: December 21, 2006

Vulnerability Issue in BrightStor ARCserve Backup

- Affected products

Corrective action	Product name	Platform	Last update
HS06-017-01	BrightStor ARCserve Backup r11.5 series, BrightStor ARCserve Backup r11.1 series, BrightStor ARCserve Backup Release 11 series, BrightStor ARCserve Backup v9 series	Windows	December 21, 2006

- Problem description

On October 23, 2006, CA announced on their Technical Support page (Japanese) that BrightStor ARCserve Backup r11.5, BrightStor ARCserve Backup r11.1, BrightStor ARCserve Backup Release 11, and BrightStor ARCserve Backup v9 have a vulnerability concerning buffer overflow.

Malicious remote users can exploit the buffer overflow vulnerability and execute arbitrary commands on backup servers that have the above products installed.

Revision history

- December 21, 2006: 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

[» 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](#)



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



Update: December 21, 2006

**HS06-017;
Vulnerability Issue in BrightStor ARCserve Backup**

Solutions for BrightStor ARCserve Backup

The vulnerability below was found in BrightStor ARCserve Backup r11.5, BrightStor ARCserve Backup r11.1, BrightStor ARCserve Backup Release 11, and BrightStor ARCserve Backup v9.

Malicious remote users can exploit the buffer overflow vulnerability and execute arbitrary commands on backup servers that have BrightStor ARCserve Backup products installed.

Please visit the CA website (Japanese) below and apply the corrective patches.
http://www.casupport.jp/resources/info/bs_security_service.htm

[Influence]

This vulnerability affects the following BrightStor ARCserve Backup products containing the CA BrightStor Backup Agent RPC Server service, CA BrightStor Job Engine service, and CA BrightStor Discovery service:

- BrightStor ARCserve Backup r11.5 series
- BrightStor ARCserve Backup r11.1 series
- BrightStor ARCserve Backup Release 11 series
- BrightStor ARCserve Backup v9 series

Please note that this vulnerability affects BrightStor ARCserve Backup r11.5 SP1 and earlier. If your system has already applied the BrightStor ARCserve Backup SP2, this vulnerability does not arise.

[Affected models, versions, and fixed versions]

BrightStor ARCserve Backup r11.5 series

CA product name	Model (*1)	Version	Patch (*2)	Platform	Last update
BrightStor ARCserve Backup r11.5 for Windows	RT-1242C-1184	11-50, 11-51			December 21, 2006
BrightStor ARCserve Backup r11.5 for Windows Agent for Lotus	RT-1242C-	11-50, 11-51			December 21, 2006

> 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



Domino	1984				
BrightStor ARCserve Backup r11.5 for Windows Agent for Microsoft Exchange	RT-1242C-1884	11-50, 11-51	QO82860.CAZ and QO83306.CAZ	Windows	December 21, 2006
BrightStor ARCserve Backup r11.5 for Windows Agent for Microsoft Exchange Premium Add-On	RT-1242C-2884	11-50, 11-51			December 21, 2006
BrightStor ARCserve Backup r11.5 for Windows Agent for Microsoft Exchange Premium Bundle	RT-1242C-3884	11-50, 11-51			December 21, 2006
BrightStor ARCserve Backup r11.5 for Windows Agent for Microsoft SQL	RT-1242C-1484	11-50, 11-51			December 21, 2006
BrightStor ARCserve Backup r11.5 for Windows Agent for Oracle	RT-1242C-1584	11-50, 11-51			December 21, 2006
BrightStor ARCserve Backup r11.5 for Windows Microsoft SQL Suite	RT-1242C-S384	11-50, 11-51			December 21, 2006
BrightStor ARCserve Backup r11.5 for Windows Microsoft Exchange Suite	RT-1242C-S484	11-50, 11-51			December 21, 2006
BrightStor ARCserve Backup r11.5 for Windows SAN Secondary Server Bundle	RT-1242C-S684	11-50, 11-51			December 21, 2006
BrightStor ARCserve Backup r11.5 Universal Client Agent for Windows	RT-1242C-2P84	11-50, 11-51			December 21, 2006
BrightStor ARCserve Backup r11.5 Universal Client Agent for 64bit Windows	RT-1242C-2Q84	11-50, 11-51			December 21, 2006

(*1) All upgrade versions and hardware-bundled versions are also affected.

(*2) These patches are provided on the CA website (Japanese).

BrightStor ARCserve Backup r11.1 series

CA product name	Model (*3)	Version	Patch (*4)	Platform	Last update
BrightStor ARCserve Backup r11.1 for Windows	RT-1242C-1174	11-10	QO82863.CAZ and	Windows	December 21, 2006
BrightStor ARCserve Backup r11.1 for Windows Agent for Lotus Domino	RT-1242C-1974	11-10			December 21, 2006
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft Exchange	RT-1242C-1874	11-10			December 21, 2006
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft Exchange Premium Add-On	RT-1242C-2874	11-10			December 21, 2006
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft Exchange Premium Bundle	RT-1242C-3874	11-10			December 21, 2006
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft SQL	RT-1242C-1474	11-10			December 21, 2006

BrightStor ARCserve Backup r11.1 for Windows Agent for Oracle	RT-1242C-1574	11-10	QO83307.CAZ		December 21, 2006
BrightStor ARCserve Backup r11.1 for Windows Microsoft SQL Suite	RT-1242C-S374	11-10			December 21, 2006
BrightStor ARCserve Backup r11.1 for Windows Microsoft Exchange Suite	RT-1242C-S474	11-10			December 21, 2006
BrightStor ARCserve Backup r11.1 for Windows SAN Secondary Server Bundle	RT-1242C-S674	11-10			December 21, 2006
BrightStor ARCserve Backup r11.1 Universal Client Agent for Windows	RT-1242C-2P74	11-10			December 21, 2006
BrightStor ARCserve Backup r11.1 Universal Client Agent for 64bit Windows	RT-1242C-2Q74	11-10			December 21, 2006

(*3) All upgrade versions and hardware-bundled versions are also affected.

(*4) These patches are provided on the CA website (Japanese).

BrightStor ARCserve Backup Release 11 series

CA product name	Model (*5)	Version	Patch (*6)	Platform	Last update
BrightStor ARCserve Backup Release 11 for Windows	RT-1242C-1174	11-00	QO82863.CAZ and QO83307.CAZ (*7)	Windows	December 21, 2006
BrightStor ARCserve Backup Release 11 for Windows Agent for Lotus Domino	RT-1242C-1974	11-00			December 21, 2006
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft Exchange	RT-1242C-1874	11-00			December 21, 2006
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft Exchange Premium Add-On	RT-1242C-2874	11-00			December 21, 2006
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft Exchange Premium Bundle	RT-1242C-3874	11-00			December 21, 2006
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft SQL	RT-1242C-1474	11-00			December 21, 2006
BrightStor ARCserve Backup Release 11 for Windows Agent for Oracle	RT-1242C-1574	11-00			December 21, 2006
BrightStor ARCserve Backup Release 11 for Windows Microsoft SQL Suite	RT-1242C-S374	11-00			December 21, 2006
BrightStor ARCserve Backup Release 11 for Windows Microsoft Exchange Suite	RT-1242C-S474	11-00			December 21, 2006
BrightStor ARCserve Backup Release 11 Client Agent for Windows	RT-1242C-1P74	11-00			December 21, 2006

BrightStor ARCserve Backup Release 11 Client Agent for 64bit Windows Server	RT-1242C-1Q74	11-00			December 21, 2006
---	---------------	-------	--	--	-------------------

(*5) All upgrade versions and hardware-bundled versions are also affected.

(*6) These patches are provided on the CA website (Japanese).

(*7) Before applying these patches, please upgrade the version to r11.1. For detailed information, please refer [the CA Technical Support page](#) (Japanese).

BrightStor ARCserve Backup v9 series

CA product name	Model (*7)	Version	Patch (*8)	Platform	Last update
BrightStor ARCserve Backup v9 for Windows Japanese	RT-1242C-1164	09-00	QO82856.CAZ, QO83308.CAZ	Windows	December 21, 2006
BrightStor ARCserve Backup v9 Agent for Lotus Notes for Windows	RT-1242C-1964	09-00			December 21, 2006
BrightStor ARCserve Backup v9 Backup Agent for MS Exchange for Windows	RT-1242C-1864	09-00			December 21, 2006
BrightStor ARCserve Backup v9 Agent for MS SQL for Windows	RT-1242C-1464	09-00			December 21, 2006
BrightStor ARCserve Backup v9 Agent for Oracle for Windows	RT-1242C-1564	09-00			December 21, 2006
BrightStor ARCserve Backup v9 Client Agent for Windows	RT-1242C-1P64	09-00			December 21, 2006
BrightStor ARCserve Backup v9 Client Agent for 64bit Windows Server	RT-1242C-1Q64	09-00			December 21, 2006

(*8) All upgrade versions are also affected.

(*9) These patches are provided on the CA website (Japanese).

Revision history

- December 21, 2006: Information about the vulnerability issue in BrightStor ARCserve Backup 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](#)