Update: June 3, 2005

Vulnerability of Buffer Overflow in BrightStor ARCserve Backup Universal Client Agent

- Affected products

Corrective action	Product name	Platform	Last update
HS05-009-01	BrightStor ARCserve Backup r11.1 series, BrightStor ARCserve Backup Release 11 series, BrightStor ARCserve Backup v9 series	Windows	June 3, 2005

- Problem description

On May 13, 2005, Computer Associates announced on their Technical Support page (Japanese) that Universal Client Agent products of BrightStor ARCserve Backup r11.1, BrightStor ARCserve Release 11, and BrightStor ARCserve v9 have a vulnerability concerning buffer overflow.
Malicious remote users can exploit the vulnerability of buffer overflow and execute arbitrary commands on backup servers with the above agent products installed.

Revision history

- June 3, 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

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

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

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: June 3, 2005

HS05-009;
Vulnerability of Buffer Overflow in BrightStor ARCserve Backup Universal Client Agent

Solution for BrightStor ARCserve Backup

The following vulnerability was found in BrightStor ARCserve Backup r11.1, BrightStor ARCserve Backup Release 11, and BrightStor ARCserve Backup v9: Malicious remote users can exploit the vulnerability of buffer overflow and execute arbitrary commands on backup servers that have agent products of BrightStor ARCserve Backup installed.
Please take the corrective actions or workarounds as mentioned below.

[Influence]

This vulnerability affects the following agent products on Windows platform:

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

[Corrective action]

Visit the Computer Associates website (Japanese) below and take the corrective action.
http://www.casupport.jp/resources/info/bs_security_agent.htm

[Affected models and versions]

BrightStor ARCserve Backup r11.1 series

Computer Associates Product	Model (*1)	Version	Patch (*2)	Platform	Last update
BrightStor ARCserve Backup r11.1 Universal Client Agent for Windows	RT-1242C-2P74	11-10	11.1	Windows	June 3, 2005
BrightStor ARCserve Backup r11.1 Universal Client Agent for 64bit Windows	RT-1242C-2Q74	11-10	11.1 64BIT		June 3, 2005
BrightStor ARCserve Backup r11.1 for Windows NDMP NAS Option	RT-1242C-1N74	11-10	11.1		June 3, 2005

BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft Exchange Premium Add-On	RT-1242C-2874	11-10	11.1		June 3, 2005
BrightStor ARCserve Backup r11.1 for Windows Agent for Oracle	RT-1242C-1574	11-10	11.1		June 3, 2005

(*1) All upgrade versions are also affected.

(*2) This is the version number for patches described in the `Solution` column of the Computer Associates website (Japanese).

BrightStor ARCserve Backup Release 11 series

Computer Associates Product	Model (*3)	Version	Patch (*4)	Platform	Last update
BrightStor ARCserve Backup Release 11 Client Agent for Windows	RT-1242C-1P74	11-00	11.0	Windows	June 3, 2005
BrightStor ARCserve Backup Release 11 Client Agent for 64bit Windows Server	RT-1242C-1Q74	11-00	11.0 64BIT		June 3, 2005
BrightStor ARCserve Backup Release 11 for Windows NDMP NAS Option	RT-1242C-1N74	11-00	11.0		June 3, 2005
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft Exchange Premium Bundle	RT-1242C-3874	11-00	11.0		June 3, 2005
BrightStor ARCserve Backup Release 11 for Windows Agent for Oracle	RT-1242C-1574	11-00	11.0		June 3, 2005

(*3) All upgrade versions are also affected.

(*4) This is the version number for patches described in the `Solution` column of the Computer Associates website (Japanese).

BrightStor ARCserve Backup v9 series

Computer Associates Product	Model (*5)	Version	Patch (*6)	Platform	Last update
BrightStor ARCserve Backup v9 Agent for Oracle for Windows	RT-1242C-1564	09-00	9.01	Windows	June 3, 2005
BrightStor ARCserve Backup v9 Client Agent for Windows	RT-1242C-1P64	09-00	9.01		June 3, 2005
BrightStor ARCserve Backup v9 Client Agent for 64bit Windows Servers	RT-1242C-1Q64	09-00	9.01 64BIT		June 3, 2005
BrightStor ARCserve Backup v9 for Linux Client Agent for Windows Servers	RT-19S2C-1P21	09-00	Linux 9.0		June 3, 2005

(*5) All upgrade versions are also affected.

(*6) This is the version number for patches described in the `Solution` column of the Computer Associates website (Japanese).

[Workarounds]

Before applying the fixed modules, carry out the following workarounds:

- Set filtering rules so that only reliable IP addresses can access the port for receiving requests (default value = 6050) that the above agent products use.

Also, the used ports can be detected by using utility programs of ARCserve Backup.

Revision history

- June 3, 2005: Information about the vulnerability of buffer overflow in BrightStor ARCserve Backup Universal Client Agent 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