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: March 14, 2005

Vulnerability in Authentication Information for Privileged Instructions of BrightStor ARCserve Backup Client Agent (UNIX/Linux)

- Affected products

Corrective action	Computer Associates Product name	Platform	Last update
HS05-005-01	BrightStor ARCserve Backup r11.1 Universal Client Agent, BrightStor ARCserve Backup Release 11 Client Agent, BrightStor ARCserve Backup v9 Client Agent, BrightStor ARCserve 7 for Linux Client Agent	AIX Linux	March 14, 2005

- Problem description

On March 4, 2005, Computer Associates released their Technical Support(Japanese) regarding the vulnerability in the authentication information for privileged instructions of BrightStor ARCserve Backup Client Agent (UNIX/Linux) that may allow invalid access with root permission for malicious remote users.
Malicious users can exploit the vulnerability and execute arbitrary commands with root permission in the above products.

Revision history

- March 14, 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

©Hitachi, Ltd. 1994, 2008. All rights reserved.

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: March 14, 2005

HS05-005;
Vulnerability in Authentication Information for Privileged Instructions of BrightStor ARCserve Backup Client Agent (UNIX/Linux)

Solution for BrightStor ARCserve Backup

The following vulnerability was found in BrightStor ARCserve Backup Client Agent (UNIX/Linux) :

- Remote users can exploit the authentication information for root-privileged instructions and execute arbitrary code with root permission.

Please take the corrective action indicated on the website of Computer Associates.

[Influence]
This vulnerability affects BrightStor ARCserve Backup Client Agent for UNIX or Linux.

[Affected models and versions]

For AIX

Product name of Computer Associates	Model (*1)	Patch (*2)	Platform	Last update
BrightStor ARCserve Backup r11.1 Universal Client Agent for UNIX	RT-1242C-2U74	AIX	AIX	March 14, 2005

(*1) Download the patch from the Computer Associates website.
BrightStor Products: BrightStor ARCserve Backup
OS: UNIX
Identified security problem: Reference the vulnerability that allows invalid access for remote users and select the corresponding patch classified by the version number in the patch list.

For Linux

Product name of Computer Associates	Model (*2)	Patch (*3)	Platform	Last update
BrightStor ARCserve Backup r11.1 Universal Client Agent for Linux	RT-1242C-2L74	11.1		March 14, 2005

BrightStor ARCserve Backup Release 11 Client Agent for Linux	RT-1242C-1L74	(*4)	Linux	March 14, 2005
BrightStor ARCserve Backup v9 Client Agent for Linux - Certified English on Japanese	RT-1242C-1L64	(*4)		March 14, 2005
BrightStor ARCserve Backup v9 for Linux Client Agent for Linux	RT-19S2C-1Q21	9.0		March 14, 2005
BrightStor ARCserve 7 for Linux Client Agent for Linux - Certified English on Japanese	RT-19S2C-1Q11	(*5)		March 14, 2005

(*2) All the upgrade versions are also affected.

(*3) Download the patch from the Computer Associates website.

BrightStor Products: BrightStor ARCserve Backup

OS: Linux

Identified security problem: Reference the vulnerability that allows invalid access for remote users and select the corresponding patch classified by the version number in the patch list.

(*4) As of March 4, 2005, this is currently under investigation by Computer Associates.

(*5) If you are not using Netstrage120, select patch 7.0.
If you are using Netstrage120, contact your Hitachi support service representative.

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

Revision history

- March 14, 2005: Information about the vulnerability in authentication information for privileged instructions of BrightStor ARCserve Backup Client Agent (UNIX/Linux) 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

| Term of Use | Privacy Notice | About Hitachi |

©Hitachi, Ltd. 1994, 2008. All rights reserved.