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: April 1, 2005

Vulnerability of Buffer Overflow in Computer Associates License Software

- Affected products

Corrective actions	Computer Associates Product name	Platform	Last update
HS05-007-01	BrightStor ARCserve Backup r11.1 series, BrightStor ARCserve Backup Release 11 series, eTrust AntiVirus 7.1 series	Windows	April 1, 2005
HS05-007-02	eTrust Access Control	HP-UX, Solaris, AIX, Red Hat Linux	April 1, 2005

- Problem description

On March 3, 2005, Computer Associates announced on their Technical Support page (Japanese) that the license patches to address buffer overflow vulnerability are available.
Malicious remote users can exploit the vulnerability of buffer overflow and execute arbitrary commands with local SYSTEM privileges in the above products.

Revision history

- April 1, 2005: This page is released.

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

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: April 1, 2005

HS05-007;
Vulnerability of Buffer Overflow in Computer Associates License Software

Solution for BrightStor ARCserve Backup/eTrust AntiVirus

The following vulnerability was found in CA License software that is included in BrightStor ARCserve Backup r11.1, BrightStor ARCserve Backup Release11, and eTrust AntiVirus 7.1:

- On backup servers, malicious remote users can exploit the vulnerability of buffer overflow and execute arbitrary commands.

Please take the corrective actions or workarounds indicated on the website of Computer Associates.

[Influence]
This vulnerability affects the Computer Associates License software that is included in BrightStor ARCserve Backup r11.1(for Windows), BrightStor ARCserve Backup Release11, and eTrust AntiVirus 7.1.
The software included in BrightStor ARCserve Backup r11.1 (for Linux) is not affected.
For details, see *Affected models and versions* below.

[Affected CA License software]
Versions between 0.1.0.15 and 0.1.4.6 of CA License Client services (`lic98rmt.exe`) of CA License software are affected.

[How to confirm the vulnerability]
Use one of the following methods to confirm whether the CA License software in your system is vulnerable or not.

1. The programs to check if your CA License software is vulnerable are available on the Computer Associates website. Execute `CalicVulnUtil.exe` (Download it from the Computer Associates website below.) at a command prompt and check the return value.
   http://www.casupport.jp/resources/info/050301security_notice.htm (Japanese)

   Vulnerable : RC=1 - system is vulnerable and must be upgraded to v1.61.9
   Invulnerable : RC=0 - system has been patched and is not vulnerable

RC=2 - system is not vulnerable but it should be upgraded

RC=3 - system does not have any version of CA licensing installed

2. Execute `lic98version.exe` at a command prompt and write the printed version number to `lic98version.log`. Check the version number of `lic98rmt.exe` written in `lic98version.log`.
   Versions from 0.1.0.15 to 0.1.4.6 are vulnerable.

3. On Windows explorer, right-click `lic98rmt.exe`, select `Properties`, and then select the `Version` tab. Check the version number of `lic98rmt.exe`.
   Versions from 0.1.0.15 to 0.1.4.6 are vulnerable.

[Corrective actions and workarounds]
Visit the Computer Associates website (Japanese) below and take the corrective action. http://www.casupport.jp/resources/info/050301security_notice.htm

Workarounds for this vulnerability exist. Both of them are provisional workarounds, so the application of the appropriate patch is recommended.

1. Check whether CA-License Client service is running in the Windows `Services` console. If the service is running, stop the service.

2. Close ports 10202, 10203, and 10204.

[Affected models and versions]

For the BrightStor ARCserve Backup r11.1 series

Computer Associates Product name	Model (*1)	Version	Platform	Last update
BrightStor ARCserve Backup r11.1 for Windows	RT-1242C-1174	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Disaster Recovery Option	RT-1242C-1A74	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Tape RAID Option	RT-1242C-1774	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Image Option	RT-1242C-1674	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Tape Library Option	RT-1242C-1374	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows SAN Option	RT-1242C-1S74	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows NDMP NAS Option	RT-1242C-1N74	11-10		April 1, 2005

BrightStor ARCserve Backup r11.1 for Windows Agent for Open Files	RT-1242C-1G74	11-10	Windows	April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft SQL	RT-1242C-1474	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft Exchange	RT-1242C-1874	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft Exchange Premium Add-On	RT-1242C-2874	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft Exchange Premium Bundle	RT-1242C-3874	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Agent for Oracle	RT-1242C-1574	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Agent for Lotus Domino	RT-1242C-1974	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Microsoft SQL Suite	RT-1242C-S374	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Microsoft Exchange Suite	RT-1242C-S474	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows SAN Secondary Server Bundle	RT-1242C-S674	11-10		April 1, 2005
BrightStor ARCserve Backup r11.1 for Windows Client for VSS software Snap-shot	RT-1242C-S774	11-10		April 1, 2005

(*1) All the upgrade versions and hard-bundle versions are also affected.

For the BrightStor ARCserve Backup Release 11 series

Computer Associates Product name	Model (*1)	Version	Platform	Last update
BrightStor ARCserve Backup Release 11 for Windows	RT-1242C-1174	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Disaster Recovery Option	RT-1242C-1A74	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Tape RAID Option	RT-1242C-1774	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Image Option	RT-1242C-1674	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Tape Library Option	RT-1242C-1374	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows SAN Option	RT-1242C-1S74	11-00		April 1, 2005
	RT-			

BrightStor ARCserve Backup Release 11 for Windows NDMP NAS Option	1242C-1N74	11-00	Windows	April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Agent for Open Files	RT-1242C-1G74	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft SQL	RT-1242C-1474	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft Exchange	RT-1242C-1874	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft Exchange Premium Add-On	RT-1242C-2874	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft Exchange Premium Bundle	RT-1242C-3874	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Agent for Oracle	RT-1242C-1574	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Agent for Lotus Domino	RT-1242C-1974	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Microsoft SQL Suite	RT-1242C-S374	11-00		April 1, 2005
BrightStor ARCserve Backup Release 11 for Windows Microsoft Exchange Suite	RT-1242C-S474	11-00		April 1, 2005

(*1) All the upgrade versions and hard-bundle versions are also affected.

For the eTrust AntiVirus 7.1 series

Computer Associates Product name	Model (*2)	Version	Platform	Last update
eTrust Antivirus r7.1 - 1 User - Includes Antivirus protection for the Desktop,Server,Gateway and Groupware	RT-1242C-2164	07-10	Windows	April 1, 2005
eTrust Antivirus r7.1 - 5 Users - Includes Antivirus protection for the Desktop,Server,Gateway and Groupware	RT-1242C-2264	07-10		April 1, 2005
eTrust Antivirus r7.1 - 10 Users - Includes Antivirus protection for the Desktop,Server,Gateway and Groupware	RT-1242C-2364	07-10		April 1, 2005
eTrust Antivirus r7.1 - 25 Users - Includes Antivirus protection for the Desktop,Server,Gateway and Groupware	RT-1242C-2464	07-10		April 1, 2005

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

Revision history

- April 1, 2005: Information about the vulnerability of buffer overflow in Computer Associates License software 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

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: April 1, 2005

HS05-007;
Vulnerability of Buffer Overflow in Computer Associates License Software

Solution for eTrust Access Control

The following vulnerability was found in CA License software that is included in eTrust Access Control:

- On servers on which eTrust Access Control is installed, malicious remote users can exploit the vulnerability of buffer overflow and execute arbitrary commands.

Please take the corrective actions or workarounds indicated on the website of Computer Associates.

[Influence]
This vulnerability affects the Computer Associates License software that is included in eTrust Access Control.
For details, see *Affected models and versions* below.

[Affected CA License software]
Versions between 0.1.0.15 and 0.1.4.6 of CA License Client services (`licrmt`) of CA License software are affected.

[How to confirm the vulnerability]
Use one of the following methods to confirm whether the CA License software in your system is vulnerable or not.

1. The programs to check if your CA License software is vulnerable are available on the Computer Associates website. Execute `CalicVulnUtil` (Download it from the Computer Associates website below.) at a command prompt and check the return value.
   http://www.casupport.jp/resources/info/050301security_notice.htm (Japanese)

   Vulnerable : RC=1 - system is vulnerable and must be upgraded to v1.61.9
   Invulnerable : RC=0 - system has been patched and is not vulnerable
   RC=2 - system is not vulnerable but it should be upgraded
   RC=3 - system does not have any version of CA licensing installed

2. Execute `lic98version` at a command prompt and write the printed

version number to `lic98version.log`. Check the version number of `licrmt` written in `lic98version.log`.
Versions from 0.1.0.15 to 0.1.4.6 are vulnerable.

3. Execute `strings licrmt | grep BUILD` at a command-prompt.
   The following string format will be returned:
   `"LICAGENT BUILD INFO=/xxx/Apr 16 2003/17:13:35"`(*xxx* indicates the file version.)
   Versions from 0.1.0.15 to 0.1.4.6 are vulnerable.

[Corrective actions and workarounds]
Visit the Computer Associates website (Japanese) below and take the corrective action. http://www.casupport.jp/resources/info/050301security_notice.htm

Workarounds for this vulnerability exist. Both of them are provisional workarounds, so the application of the appropriate patch is recommended.

1. Check whether CA-License Client (licrmt) is running. If CA-License Client is running, stop CA-License Client.

2. Close ports 10202, 10203, and 10204.

[Affected models and versions]

For eTrust Access Control

Computer Associates Product name	Model	Version	Platform	Last update
eTrust Access Control	RT-1V28-AC99002*n* (*1)	05-30	HP-UX	April 1, 2005
		05-30	Solaris	April 1, 2005
		05-30	AIX	April 1, 2005
		05-30	Red Hat Linux	April 1, 2005

(*1) "*n*" is a placeholder for 0 to 9.

Revision history

- April 1, 2005: Information about vulnerability of buffer overflow in Computer Associates License software is released.

- 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