トップ

What's New

お知らせ

御参考（警告情報など）

ソフトウェア製品セキュリティ情報

セキュリティ対応機関へのリンク

お問い合わせ

soft-security
@itg.hitachi.co.jp

2005.03.25更新

CAライセンスソフトウエアのバッファオーバーフロー攻撃に関するセキュリティ問題

- 影響がある製品

対策	コンピュータ・アソシエイツ社製品群	適用ＯＳ	更新日
HS05-007-01	BrightStor ARCserve Backup r11.1 シリーズ、 BrightStor ARCserve Backup Release 11 シリーズ、 eTrust AntiVirus 7.1 シリーズ	Windows	2005.03.22
HS05-007-02	eTrust Access Control	HP-UX、Solaris、AIX、Red Hat Linux	2005.03.25

- 問題の説明

2005.03.03、コンピュータ・アソシエイツ(CA)社Technical Supportにてバッファ・オーバーフロー対策用ライセンス・パッチのお知らせが公表されました。
上記の製品において、外部から悪意のあるユーザによるバッファオーバーフロー攻撃を受けることで、ローカルシステム特権で任意のコマ

ンドを実行できる脆弱性があります。

更新履歴 ：

- 2005.03.25 : 影響がある製品、HS05-007-02を追加し、問題の説明を更新しました。
- 2005.03.22 : このセキュリティ情報ページを新規作成および発信しました。

- 弊社では，セキュリティ対応に関して正確な情報を提供するよう努力しておりますが，セキュリティ問題に関する情報は変化しており，当ホームページで記載している内容を予告なく変更することがありますので，あらかじめご了承ください。情報ご参照の際には，常に最新の情報をご確認いただくようお願いします。
- 当ホームページに記載されている製品には，他社開発製品が含まれております。これらのセキュリティ情報については他社から提供，または公開された情報を基にしております。弊社では，情報の正確性および完全性について注意を払っておりますが，開発元の状況変化に伴い，当ホームページの記載内容に変更が生じることがあります。
- 当ホームページはセキュリティ情報の提供を目的としたものであり，法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ

¦ サイトの利用条件 ¦ 個人情報保護ポリシー ¦ 日立について ¦

トップ
What's New
お知らせ
御参考（警告情報など）
ソフトウェア製品セキュリティ情報
セキュリティ対応機関へのリンク

お問い合わせ
soft-security
@itg.hitachi.co.jp

2005.03.22更新

HS05-007;
CAライセンスソフトウエアのバッファオーバーフロー攻撃に関するセキュリティ問題

BrightStor ARCserve Backup/eTrust AntiVirusの対策

BrightStor ARCserve Backup r11.1、BrightStor ARCserve Backup Release11および、eTrust AntiVirus7.1に含まれているCAライセンスソフトウェアに次のセキュリティ上の問題があることが判明しました。
バックアップサーバにおいて、外部から悪意のあるユーザによるバッファオーバーフロー攻撃を受けることで、任意のコマンドを実行することができる脆弱性があります。
つきましては、コンピュータ・アソシエイツ社のホームページをご参照いただき対策または暫定回避策をお願いします。

[影響範囲]
BrightStor ARCserve Backup r11.1(Windows版)、BrightStor ARCserve Backup Release11、eTrust AntiVirus 7.1に含まれているCAライセンスソフトウェアの問題です。
BrightStor ARCserve Backup r11.1(Linux版)は該当しません。

該当製品名の詳細は、[該当するCAライセンスソフトウェアが含まれている製品名・バージョン]をご参照願います。

[該当するCAライセンスソフトウェア]

CAライセンスソフトウェアのCA License Clientサービス（lic98rmt.exe）のバージョンが、0.1.0.15 から 0.1.4.6 の間の場合、該当します。

[確認方法]

次のいずれかの方法で脆弱性の有無を確認して下さい。

1. コンピュータ・アソシエイツ社 Webにてライセンスセキュリティパッチ適用の有無を判断するユーティリティの提供をおこなっております。コマンドプロンプトからCalicVulnUtil.exe（コンピュータ・アソシエイツ社Webよりダウンロード）を実行し、リターンコードにより確認可能です。

   http://www.casupport.jp/resources/info/050301security_notice.htm

   「脆弱性診断ツールはこちら」または「このセキュリティパッチに関するFAQはこちら」から項番23『サーバが脆弱であるかどうかを調べるために使用できるプログラムはありますか？』をご確認ください。

   脆弱性あり : RC=1 - system is vulnerable and must be upgraded to v1.61.9

   脆弱性なし : 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. コマンドプロンプトからlic98version.exeを起動し、バージョン番号をlic98version.logへ書き込んだ後、lic98version.logへ書き込まれたlic98rmt.exeのバージョンを確認します。

   0.1.0.15 から 0.1.4.6 の間であれば脆弱性ありに該当します。

3. エクスプローラでlic98rmt.exeを右クリックしてプロパティを選び、次にバージョンタブを選んで、lic98rmt.exeのバージョンを確認します。
   0.1.0.15 から 0.1.4.6 の間であれば脆弱性ありに該当します。

[対策及び暫定回避策]
コンピュータ・アソシエイツ社の以下のホームページを参照し、対策パッチの適用をお願いします。
http://www.casupport.jp/resources/info/050301security_notice.htm

またこの脆弱性に対して下記暫定回避策があります。どちらも一時的な回避策となりますので、対策パッチの適用をお願いします。

1. Windowsのサービス画面を使って「CA-License Client」というサービスが起動しているかどうかをチェックし、起動していれば停止／無効にしておきます。
   詳細は、コンピュータ・アソシエイツ社ページから「このセキュリティパッチに関するFAQはこちら」をクリックし、項番4『ファイアウォールが原因でパッチをダウンロードできない場合はどうすればよいですか？』をご参照ください。

2. ポート10202、10203および10204を閉じておきます。
   詳細は、コンピュータ・アソシエイツ社ページから「このセキュリティパッチに関するFAQはこちら」をクリックし、項番9『企業ファイアウォールの外部でサーバを稼動させています。この脆弱性の影響を受けるポートはどれですか？』をご参照ください。

[該当するCAライセンスソフトウェアが含まれている製品名・バージョン]

BrightStor ARCserve Backup r11.1 シリーズ

コンピュータ・アソシエイツ社の製品名	形名(注1)	対象バージョン	適用ＯＳ	更新日
BrightStor ARCserve Backup r11.1 for Windows	RT-1242C-1174	11-10	Windows	2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Disaster Recovery Option	RT-1242C-1A74	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Tape RAID Option	RT-1242C-1774	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Image Option	RT-1242C-1674	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Tape Library Option	RT-1242C-1374	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows SAN Option	RT-1242C-1S74	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows NDMP NAS Option	RT-1242C-1N74	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Agent for Open Files	RT-1242C-1G74	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft SQL	RT-1242C-1474	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft Exchange	RT-1242C-1874	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft Exchange	RT-1242C-	11-10		2005.03.22

Premium Add-On	2874			
BrightStor ARCserve Backup r11.1 for Windows Agent for Microsoft Exchange Premium Bundle	RT-1242C-3874	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Agent for Oracle	RT-1242C-1574	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Agent for Lotus Domino	RT-1242C-1974	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Microsoft SQL Suite	RT-1242C-S374	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Microsoft Exchange Suite	RT-1242C-S474	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows SAN Secondary Server Bundle	RT-1242C-S674	11-10		2005.03.22
BrightStor ARCserve Backup r11.1 for Windows Client for VSS software Snap-shot	RT-1242C-S774	11-10		2005.03.22

(注1) 各アップグレード版および、各ハードバンドル版も対象となります。

BrightStor ARCserve Backup Release 11 シリーズ

コンピュータ・アソシエイツ社の製品名	形名 (注1)	対象バージョン	適用ＯＳ	更新日
BrightStor ARCserve Backup Release 11 for Windows	RT-1242C-1174	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows Disaster Recovery Option	RT-1242C-1A74	11-00		2005.03.22
	RT-			

BrightStor ARCserve Backup Release 11 for Windows Tape RAID Option	1242C-1774	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows Image Option	RT-1242C-1674	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows Tape Library Option	RT-1242C-1374	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows SAN Option	RT-1242C-1S74	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows NDMP NAS Option	RT-1242C-1N74	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows Agent for Open Files	RT-1242C-1G74	11-00	Windows	2005.03.22
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft SQL	RT-1242C-1474	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft Exchange	RT-1242C-1874	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft Exchange Premium Add-On	RT-1242C-2874	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows Agent for Microsoft Exchange Premium Bundle	RT-1242C-3874	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows Agent for Oracle	RT-1242C-1574	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows Agent for Lotus Domino	RT-1242C-1974	11-00		2005.03.22

BrightStor ARCserve Backup Release 11 for Windows Microsoft SQL Suite	RT-1242C-S374	11-00		2005.03.22
BrightStor ARCserve Backup Release 11 for Windows Microsoft Exchange Suite	RT-1242C-S474	11-00		2005.03.22

(注1) 各アップグレード版および、各ハードバンドル版も対象となります。

eTrust AntiVirus 7.1 シリーズ

コンピュータ・アソシエイツ社の製品名	形名 (注2)	対象バージョン	適用ＯＳ	更新日
eTrust Antivirus r7.1 - 1 User - Includes Antivirus protection for the Desktop,Server,Gateway and Groupware	RT-1242C-2164	07-10	Windows	2005.03.22
eTrust Antivirus r7.1 - 5 Users - Includes Antivirus protection for the Desktop,Server,Gateway and Groupware	RT-1242C-2264	07-10		2005.03.22
eTrust Antivirus r7.1 - 10 Users - Includes Antivirus protection for the Desktop,Server,Gateway and Groupware	RT-1242C-2364	07-10		2005.03.22
eTrust Antivirus r7.1 - 25 Users - Includes Antivirus protection for the Desktop,Server,Gateway and Groupware	RT-1242C-2464	07-10		2005.03.22

(注2) 各アップグレード版も対象となります。

更新履歴 ：

- 2005.03.22 : CAライセンスソフトウエアのバッファオーバーフロー攻撃に関するセキュリティ問題の情報を公開しました。

- 弊社では，セキュリティ対応に関して正確な情報を提供するよう努力して

おりますが，セキュリティ問題に関する情報は変化しており，当ホームページで記載している内容を予告なく変更することがありますので，あらかじめご了承ください。情報ご参照の際には，常に最新の情報をご確認いただくようお願いします。

- 当ホームページに記載されている製品には，他社開発製品が含まれております。これらのセキュリティ情報については他社から提供，または公開された情報を基にしております。弊社では，情報の正確性および完全性について注意を払っておりますが，開発元の状況変化に伴い，当ホームページの記載内容に変更が生じることがあります。
- 当ホームページはセキュリティ情報の提供を目的としたものであり，法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ

ソフトウェア製品セキュリティ情報
Software Vulnerability Information

ソフトウェア事業部 (Software Division)

2005.03.25更新

HS05-007;

CAライセンスソフトウエアのバッファオーバーフロー攻撃に関するセキュリティ問題

eTrust Access Controlの対策

eTrust Access Controlに含まれているCAライセンスソフトウェアに次のセキュリティ上の問題があることが判明しました。

eTrust Access Controlをインストールしているサーバにおいて、外部から悪意のあるユーザによるバッファオーバーフロー攻撃を受けることで、任意のコマンドを実行することができる脆弱性があります。

つきましては、コンピュータ・アソシエイツ社のホームページをご参照いただき対策または暫定回避策をお願いします。

[影響範囲]

eTrust Access Controlに含まれているCAライセンスソフトウェアの問題です。

該当製品名の詳細は、[該当するCAライセンスソフトウェアが含まれている製品名・バージョン]をご参照願います。

トップ
What's New
お知らせ
御参考（警告情報など）
ソフトウェア製品セキュリティ情報
セキュリティ対応機関へのリンク

お問い合わせ
soft-security
@itg.hitachi.co.jp

[該当するCAライセンスソフトウェア]

CAライセンスソフトウェアのCA License Clientサービス（licrmt）のバージョンが、0.1.0.15 から 0.1.4.6 の間の場合、該当します。

[確認方法]

次のいずれかの方法で脆弱性の有無を確認して下さい。

1. コンピュータ・アソシエイツ社 Webにてライセンスセキュリティパッチ適用の有無を判断するユーティリティの提供をおこなっております。コマンドプロンプトからCalicVulnUtil（コンピュータ・アソシエイツ社Webよりダウンロード）を実行し、リターンコードにより確認可能です。

   http://www.casupport.jp/resources/info/050301security_notice.htm

   「脆弱性診断ツールはこちら」または「このセキュリティパッチに関するFAQはこちら」から項番23『サーバが脆弱であるかどうかを調べるために使用できるプログラムはありますか？』をご確認ください。

   脆弱性あり : RC=1 - system is vulnerable and must be upgraded to v1.61.9

   脆弱性なし : 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. コマンドプロンプトからlic98versionを起動し、バージョン番号をlic98version.logへ書き込んだ後、lic98version.logへ書き込まれたlicrmtのバージョンを確認します。

   0.1.0.15 から 0.1.4.6 の間であれば脆弱性ありに該当します。

3. コマンドプロンプトからstrings licrmt ¦ grep BUILDを実行すると、次のようなストリングフォーマットが戻ってきます。

"LICAGENT BUILD INFO=/xxx/Apr 16 2003/17:13:35"(xxxはバージョン番号を示します。)バージョンを確認します。

0.1.0.15 から 0.1.4.6 の間であれば脆弱性ありに該当します。

[対策及び暫定回避策]

コンピュータ・アソシエイツ社の以下のホームページを参照し、対策パッチの適用をお願いします。

http://www.casupport.jp/resources/info/050301security_notice.htm

またこの脆弱性に対して下記暫定回避策があります。どちらも一時的な回避策となりますので、対策パッチの適用をお願いします。

1. CA License Client(licrmt)が起動しているかどうかをチェックし、起動していれば停止しておきます。

2. ポート10202、10203および10204を閉じておきます。
   詳細は、コンピュータ・アソシエイツ社ページから「このセキュリティパッチに関するFAQはこちら」をクリックし、項番9『企業ファイアウォールの外部でサーバを稼動させています。この脆弱性の影響を受けるポートはどれですか？』をご参照ください。

[該当するCAライセンスソフトウェアが含まれている製品名・バージョン]

eTrust Access Control

コンピュータ・アソシエイツ社の製品名	形名	対象バージョン	適用ＯＳ	更新日
eTrust Access Control	RT-1V28-AC99002n (注1)	05-30	HP-UX	2005.03.25
		05-30	Solaris	2005.03.25
		05-30	AIX	2005.03.25
		05-30	Red Hat Linux	2005.03.25

(注1) nには数字0～9が入ります。

更新履歴 ：

- 2005.03.25 : CAライセンスソフトウエアのバッファオーバーフロー攻撃に関するセキュリティ問題の情報を公開しました。

- 弊社では，セキュリティ対応に関して正確な情報を提供するよう努力しておりますが，セキュリティ問題に関する情報は変化しており，当ホームページで記載している内容を予告なく変更することがありますので，あらかじめご了承ください。情報ご参照の際には，常に最新の情報をご確認いただくようお願いします。
- 当ホームページに記載されている製品には，他社開発製品が含まれております。これらのセキュリティ情報については他社から提供，または公開された情報を基にしております。弊社では，情報の正確性および完全性について注意を払っておりますが，開発元の状況変化に伴い，当ホームページの記載内容に変更が生じることがあります。
- 当ホームページはセキュリティ情報の提供を目的としたものであり，法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ