Cisco ACE アプリケーション コントロール エンジン モジュールおよび Cisco ACE 4710 アプリケーション コントロール エンジンの多重 脆弱点

Critical

アドバイザリーID : cisco-sa-20090225-ace

初公開日 : 2009-02-25 16:00

バージョン 1.1 : Final

CVSSスコア : 10.0

回避策 : Yes

Cisco バグ ID :

CVE-2009-0620
CVE-2009-0624
CVE-2009-0623
CVE-2009-0622
CVE-2009-0621
CVE-2009-0625

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

不正利用される、次の影響の何れかという結果に終る場合がある場合、Cisco ACE アプリケーション コントロール エンジン モジュールおよび Cisco ACE 4710 アプリケーション コントロール エンジンは多重 脆弱点が含まれています:

- デフォルトユーザ名およびパスワードによる管理上の水平なアクセス
- 特権 拡大
- サービス拒否 （ DoS ）状態

Cisco は影響を受けた顧客向けに利用可能 な フリーソフト アップデートをリリースしました。いくつかの脆弱性を軽減する回避策は利用できます。

注: これらの脆弱性は相互に関連していません。 ある機器が 1 つの脆弱性の影響を受け、他の脆弱性の影響は受けない場合もあります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090225-ace で掲示されます。

注: このアドバイザリは Cisco 4700 シリーズ アプリケーション コントロール エンジン デバイス マネージャおよび Application Networking Manager モジュールソフトウェアに影響を与える多重脆弱点発表アドバイザリと同時にリリースされています。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090225-anm で掲示されます

該当製品

修正済みソフトウェア

次 の テーブルはこのアドバイザリの内で記述されている各脆弱性から影響を受ける製品を表示する。

脆弱性	影響を受ける製品およびバージョン	
	Cisco ACE 4710 アプライアンス	Cisco ACE モジュール
デフォルトのユーザ名およびパスワード	A1(8a) 以前のすべてのバージョン	A2(1.1) 以前のすべてのバージョン
特権 拡大脆弱性	A1(8a) 以前のすべてのバージョン	A2(1.2) 以前のすべてのバージョン
巧妙に細工された SSH パケットの脆弱性	A3(2.1) 以前のすべてのバージョン	A2(1.3) 以前のすべてのバージョン
細工 された Simple Network Management Protocol (SNMP) バージョン 2 (SNMPv2) パケットの脆弱性	A3(2.1) 以前のすべてのバージョン	A2(1.3) 以前のすべてのバージョン
巧妙に細工された SNMPv3 パケットの脆弱性	A1(8.0) 以前のすべてのバージョン	A2(1.2) 以前のすべてのバージョン

ソフトウェア バージョンの判別

現在 ACE アプリケーション コントロール エンジンを on Cisco 実行しているシステム ソフトウェアのバージョンを表示するために、**show version コマンドを**使用して下さい。 次の例は Cisco ACE アプリケーション コントロール エンジンソフトウェア バージョン A3(1.0) の **show version コマンド**の出力を表示するものです:

```
ACE-4710/Admin# show version
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 1985-2008 by Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:    Version 0.95
  system:    Version A3(1.0) [build 3.0(0)A3(0.0.148) adbuild_03:31:25-
2008/08/06_/auto/adbure_nightly2/nightly_rel_a3_1_0_throttle/REL_3_0_0_A3_0_0
  system image file: (nd)/192.168.65.31/scimitar.bin

  Device Manager version 1.1 (0) 20080805:0415

...
<output truncated>
```

次の例は Cisco ACE アプリケーション コントロール エンジン モジュールソフトウェア バージョン A1(1) の **show version コマンド**の出力を表示するものです:

```
ACE-mod/Admin# show version
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2006, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:    Version 12.2[117]
  system:    Version 3.0(0)A1(1) [build 3.0(0)A1(1) _01:26:21-2006/03/13_/auto/adbu-
rel/ws/REL_3_0_0_A1_1]

  system image file: [LCP] disk0:c6ace-t1k9-mzg.3.0.0_A1_1.bin
  licensed features: no feature license is installed
...
<output truncated>
```

脆弱性を含んでいないことが確認された製品

Cisco ACE XML Gateway、Cisco ACE Web Application Firewall および Cisco ACE GSS 4400 シリーズ グローバル サイト セレクタ アプライアンスはこのアドバイザリに説明がある脆弱性の何れかから影響を受けません。 他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

改訂履歴

リビジョン 1.1	2009-March-09	*巧妙に細工された SNMPv2c パケットの脆弱性* セクションの SNMPv2c パケットについての明白にされた情報。 *デフォルトのユーザ名およびパスワード* セクションの*パスワード* 引数についての修正された情報。
リビジョン 1.0	2009-February-25	初版リリース

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。