Cisco ACE Application Control EngineモジュールおよびCisco ACE 4710 Application Control Engineの複数の脆弱性

High

アドバイザリーID : cisco-sa-20100811-ace
初公開日 : 2010-08-11 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2010-2825
CVE-2010-2824
CVE-2010-2823
CVE-2010-2822

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

Cisco ACE Application Control EngineモジュールおよびCisco ACE 4710 Application Control Engineには、次のDoS脆弱性が存在します。

- リアルタイムストリーミングプロトコル(RTSP)インスペクションに関するDoS脆弱性
- HTTP、RTSP、およびSession Initiation Protocol(SIP)インスペクションに関するDoS脆弱性
- Secure Socket Layer(SSL)のDoS脆弱性
- SIPインスペクションDoSの脆弱性

シスコは、該当するお客様向けに無償のソフトウェアアップデートをリリースしました。一部の脆弱性に対しては回避策があります。

注：これらの脆弱性は互いに独立しています。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、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100811-ace で公開されています。

該当製品

脆弱性のある製品

Cisco ACE Application Control EngineモジュールとCisco ACE 4710 Application Control

Engineは、複数の脆弱性の影響を受けます。影響を受けるバージョンは、脆弱性によって異なります。個々のバージョン情報については、このアドバイザリの「ソフトウェア バージョンおよび修正」セクションを参照してください。

RTSPインスペクションのDoS脆弱性

RTSPインスペクションが設定されているCisco ACE Application Control Engineモジュールおよびcisco ACE 4710 Application Control Engineアプライアンスが影響を受けます。RTSPインスペクションはデフォルトで無効になっています。

HTTP、RTSP、およびSIPインスペクションに関するDoS脆弱性

HTTP、RTSP、またはSIPインスペクションが設定されているCisco ACE 4710 Application Control Engineアプライアンスが影響を受けます。HTTP、RTSP、およびSIPインスペクションはデフォルトで無効になっています。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は、この脆弱性の影響を受けません。

注：この脆弱性は、このアドバイザリに記載されている他のRSTPおよびSIPインスペクションの脆弱性とは無関係です。

SSL DoS脆弱性

SSLトランザクションを処理するCisco ACE Application Control Engineモジュールは、この脆弱性の影響を受けます。Cisco ACE 4710 Application Control Engineアプライアンスはこの脆弱性の影響を受けません。

SIPインスペクションのDoS脆弱性

SIPインスペクションが設定されているCisco ACE Application Control Engineモジュールおよびcisco ACE 4710 Application Control Engineアプライアンスが影響を受けます。SIPインスペクションはデフォルトで無効になっています。

ソフトウェアバージョンの確認

Cisco ACE Application Control Engineで現在実行されているシステムソフトウェアのバージョンを表示するには、show versionコマンドを使用します。次の例は、Cisco ACE Application Control Engine(ACE)ソフトウェアバージョンA3(1.0)でのshow versionコマンドの出力を示しています。

```
<#root>

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)]
  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 Application Control Engine(ACE)モジュールソフトウェアバージョンA2(3.0)でのshow versionコマンドの出力を示しています。

```
<#root>

ACEmod/Admin#

 show version

Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, 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[121]
  system:    Version A2<3.0> [build 3.0(0)A2(2.99.80)]
  system image file: [LCP] disk0:c6ace-t1k9-mzg.A2_2_99_80.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記載されている脆弱性の影響を受けません。

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。

詳細

Cisco ACE 4710 Application Control EngineアプライアンスおよびCisco ACE Application Control Engineモジュール（Cisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用）は、データセンター向けのロードバランシングおよびアプリケーション配信ソリューションです。両方の製品に複数の脆弱性が存在します。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。次に、このアドバイザリで説明されている各脆弱性の詳細を示します。

RTSPインスペクションのDoS脆弱性

RTSPは、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、およびCisco IP/TV接続で使用されます。RTSPアプリケーションは、TCPおよびUDPを制御チャネルとして使用するwell-knownポート554を使用します。モジュールとアプライアンスは、RTSP over TCPのみをサポートしています。

Cisco ACE Application Control EngineモジュールおよびCisco ACE 4710 Application Control Engineには、DoS脆弱性が存在します。この脆弱性は、認証されていない攻撃者によって、巧妙に細工されたRTSPパケットが送信されることで不正利用される可能性があります。この脆弱性に該当するのは、RTSPインスペクションが有効になっているデバイスだけです。RTSPインスペクションはデフォルトで無効になっています。

注：この脆弱性を不正利用するには、TCP 3ウェイハンドシェイクが必要です。この脆弱性は通過トラフィックによってのみ引き起こされます。影響を受けるデバイス宛てのトラフィックはこの脆弱性を引き起こしません。

この脆弱性は、次のCisco Bug IDとして文書化され、Common Vulnerability and Exposures(CVE)IDが割り当てられています。

- Cisco ACE Application Control Engineアプライアンス：CSCta85227(登録ユーザ専用):CVE-2010-2822
- Cisco ACE Application Control Engineモジュール：CSCtg14858(登録ユーザ専用):CVE-2010-2822

HTTP、RTSP、およびSIPインスペクションに関するDoS脆弱性

ACEは、HTTPプロトコルのステートフルディープパケットインスペクションを実行します。ディープパケットインスペクションは、ACEがパケットまたはトラフィックストリームのアプリケーションペイロードを検査し、データの内容に基づいて決定を行う、アプリケーション検査の特殊なケースです。HTTPディープインスペクション中、アプリケーションインスペクションプロセスの主な焦点は、HTTPヘッダー、URL、および限られた範囲でのペイロードなどのHTTP属性にあります。ユーザ定義の正規表現を使用して、ペイロード内の「シグニチャ」を検出することもできます。

Cisco ACE 4710 Application Control EngineにはDoS脆弱性が存在し、巧妙に細工されたHTTPパケットを送信する際に、認証されていない攻撃者によって悪用される可能性があります。HTTP、RTSP、またはSIPインスペクションが有効になっているデバイスが影響を受けます。HTTP、RTSP、およびSIPインスペクションはデフォルトで無効になっています。

注：Cisco ACE Application Control Engineモジュールは、この脆弱性の影響を受けません。この脆弱性を不正利用するには、TCP 3ウェイハンドシェイクが必要です。この脆弱性は通過トラフィックによってのみ引き起こされます。影響を受けるデバイス宛てのトラフィックはこの脆弱性を引き起こしません。

この脆弱性は、Cisco Bug ID CSCtb54493 (登録ユーザ専用)として文書化され、CVE IDとしてCVE-2010-2823が割り当てられています。

SSL DoS脆弱性

Cisco ACE Application Control Engineモジュールには、一連のSSLパケットの送信中に認証されていない攻撃者によって不正利用される可能性のあるDoS脆弱性が含まれています。Cisco ACE 4710 Application Control Engineアプライアンスはこの脆弱性の影響を受けません。

注：この脆弱性を不正利用するには、TCP 3ウェイハンドシェイクが必要です。この脆弱性は、該当デバイス宛てのトラフィックによってのみ引き起こされます。通過トラフィックではこの脆弱性は引き起こされません。

注：Cisco ACE 4710 Application Control Engineアプライアンスは、この脆弱性の影響を受けません。

この脆弱性は、Cisco Bug ID CSCta20756 (登録ユーザ専用)として文書化され、CVE IDとしてCVE-2010-2824が割り当てられています。

SIPインスペクションのDoS脆弱性

SIPは、コール処理セッション、特に二者間の会議に使用されます。Cisco ACE Application Control EngineモジュールおよびCisco ACE 4710 Application Control Engineには、DoS脆弱性が存在します。この脆弱性は、巧妙に細工されたSIPパケットを送信する一方で、認証されていない攻撃者によって不正利用される可能性があります。SIPインスペクションが有効になっているデバイスのみが影響を受けます。SIPインスペクションはデフォルトで無効になっています。

注：TCPまたはUDP SIPパケットが原因でデバイスがリロードされることがあります。TCPが使用されている場合、この脆弱性を不正利用するにはTCP 3ウェイハンドシェイクが必要です。この脆弱性は通過トラフィックによってのみ引き起こされます。影響を受けるデバイス宛てのトラフィックはこの脆弱性を引き起こしません。

この脆弱性は、次のCisco Bug IDとして文書化され、次のCVE IDが割り当てられています。

- Cisco ACE Application Control Engineモジュール：CSCta65603(登録ユーザ専用):CVE-2010-2825
- Cisco ACE Application Control Engineアプライアンス：CSCta71569(登録ユーザ専用):CVE-2010-2825

回避策

次に示す推奨事項の他に、ネットワーク内のCiscoデバイスに適用可能な緩和テクニックが、このアドバイザリに関連するCisco適用対応策速報(https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20100811-ace)で公開されています。

RTSPインスペクションのDoS脆弱性

この脆弱性は、不要な場合はRTSPインスペクションを無効にすることで軽減できます。RTSPインスペクションはデフォルトで無効になっています。管理者は、該当するポリシーマップでno inspect rtspコマンドを発行することにより、RTSP検査を無効にすることができます。

注：この回避策は、RTSPインスペクションがロードバランシング展開で必要ない場合、または必要ない場合にのみ実行可能です。

HTTP、RTSP、およびSIPインスペクションに関するDoS脆弱性

この脆弱性は、HTTP、RTSP、およびSIPインスペクションが不要な場合にそれらを無効にすることで軽減できます。HTTP、RTSP、およびSIPインスペクションはデフォルトで無効になっています。

管理者は、該当するポリシーマップでno inspect httpコマンドを発行することにより、HTTPインスペクションを無効にすることができます。

管理者は、該当するポリシーマップでno inspect rtspコマンドを発行することにより、RTSP検査を無効にすることができます。

管理者は、該当するポリシーマップでno inspect sipコマンドを発行することにより、SIPインスペクションを無効にすることができます。

注：この回避策は、ロードバランシングの導入でHTTP、RTSP、およびSIPインスペクションが不要または必要ない場合にのみ有効です。

SSL DoS脆弱性

この脆弱性を軽減する回避策はありません。

SIPインスペクションのDoS脆弱性

この脆弱性は、不要な場合はSIPインスペクションを無効にすることで軽減できます。SIPインス

ペクションはデフォルトで無効になっています。管理者は、該当するポリシーマップでno inspect sipコマンドを発行することにより、SIPインスペクションを無効にすることができます。

注：この回避策は、ロードバランシングの導入でSIPインスペクションが不要または必要ない場合にのみ有効です。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

以下のソフトウェアテーブルの各行は、修正を含む最初のリリースを示しています（該当する場合は、それぞれのリリース予定日も記載しています）。この表の「最初の修正リリース」列に、修正を含む最初のリリースが記載されています。「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

脆弱性	First Fixed Release（修正された最初のリリース）		推奨リリース	
	ACEアプライアンス	ACEモジュール	ACEアプライアンス	ACEモジュール
RTSPインスペクションの脆弱性	A3(2.6)	A2(3.2)	A3(2.6)	A2(3.2)
HTTP、RTSP、	A3(2.6)	脆弱性なし	A3(2.6)	A2(3.2)

SIPインスペクションの脆弱性				
SSLの脆弱性	脆弱性なし	A2(1.6) A2(2.3) A2(3.1)	A3(2.6)	A2(3.2)
SIPインスペクションの脆弱性	A3(2.4)	A2(1.6) A2(2.3) A2(3.1)	A3(2.6)	A2(3.2)

Cisco ACE 4710 Application Control Engineアプライアンスソフトウェアは、次のサイトからダウンロードできます。

https://sec.cloudapps.cisco.com/support/downloads/go/Redirect.x?mdfid=281222179 (登録ユーザ専用)

Cisco ACEモジュールソフトウェアは、次の場所からダウンロードできます。

https://sec.cloudapps.cisco.com/support/downloads/go/Redirect.x?mdfid=280557289 (登録ユーザ専用)

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

これらの脆弱性は、お客様からのサービスリクエストのトラブルシューティングと内部テストの際に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100811-ace

改訂履歴

リビジョン 1.0	2010年8月11日	初回公開リリース

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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。