ACNSのDoS脆弱性とデフォルトの管理者パスワード

severity

アドバイザリーID : cisco-sa-20050224-acnsdos

初公開日 : 2005-02-24 16:00

バージョン 1.0 : Final

回避策 : No Workarounds available

Cisco バグ ID :

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 Application and Content Networking System(ACNS)ソフトウェアを実行しているデバイスは、Denial of Service(DoS)攻撃に対して脆弱で、管理者アカウントのデフォルトパスワードが含まれている場合があります。ACNSソフトウェアを実行しているデバイスは、トランスペアレントプロキシサーバ、フォワードプロキシサーバ、またはリバースプロキシサーバとして設定されている場合、DoS攻撃に対して脆弱になる可能性があります。シスコは、該当するお客様すべてに対してDoS脆弱性に対処する無償ソフトウェアを提供しています。管理アカウントのデフォルトパスワードは、ソフトウェアのアップグレードを必要とせず、該当するすべてのユーザに対して設定コマンドを実行することで変更できます。2つの脆弱性の影響を軽減する回避策があります。

この脆弱性は、次のCisco Bug IDに記載されています。

- CSCef27476(登録ユーザ専用)
- CSCef30460(登録ユーザ専用)
- CSCeg49648(登録ユーザ専用)
- CSCeg23731(登録ユーザ専用)
- CSCef30743(登録ユーザ専用)

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050224-acnsdos で公開されています。

該当製品

脆弱性のある製品

DDTSバグID	脆弱性のあるACNSバージョン
CSCef27476	リリース5.0.17.6より前の5.0
	リリース5.1.11.6より前の5.1
CSCef30460	すべての4.Xリリース
	すべての5.0リリース
	リリース5.1.11.6より前の5.1
CSCeg49648	すべての5.1リリース
CSCeg23731	すべての5.0リリース
	リリース5.1.13.7より前の5.1
	リリース5.2.3.9より前の5.2
CSCef30743	すべての4.Xリリース
	すべての5.0リリース
	すべての5.1リリース
	すべての5.2リリース

ACNSをサポートするハードウェアモデルは次のとおりです。

- Cisco 500 シリーズ Content Engine
- Cisco 7300 シリーズ Content Engine
- Ciscoコンテンツルータ4400シリーズ
- Cisco Content Distribution Manager 4600 シリーズ
- Cisco 2600、2800、3600、3700、および3800シリーズサービス統合型ルータ向けCisco Content Engineモジュール

サポートされているデバイスで実行されているACNSソフトウェアを確認するには、デバイスにログインし、**show version**コマンドを発行してシステムバナーを表示します。Cisco ACNSソフトウェアは、「アプリケーションおよびコテンツットネットワーキングシステムソフトウェア(ACNS)」と呼ばれます。著作権情報の下に、ACNSのリリースおよびビルド情報が表示されます。

次の例は、ACNSソフトウェアリリース5.1.5.2を実行しているシスコデバイスを示しています。

```
Application and Content Networking System Software (ACNS)

Copyright 1999-2003 by Cisco Systems, Inc.

Application and Content Networking System Software Release 5.1.5 (build b2 Mar 30 2004)
```

デバイスからのリリースおよびビルド情報と、このアドバイザリに記載されCCOから入手できるソフトウェアリリース情報を照合するには、リリースにビルドコードを追加し、小文字の「b」をドットに置き換えます（例：5.1.5b2は5.1.5.2になります）

脆弱性を含んでいないことが確認された製品

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

ACNSソフトウェアは、Webアプリケーションの高速化およびキャッシングサービスを提供します。Cisco ACNSソフトウェアは、デマンドプルキャッシング、プレポジショニング、ライブおよびオンデマンドストリーミングのテクノロジーを組み合わせて、Webアプリケーション、オブジェクトファイル、ライブイベント、およびビデオの配信を高速化します。Javaアプレット、Flashアニメーション、Shockwaveプログラム、その他のファイル形式など、帯域幅を大量に消費するコンテンツオブジェクトを管理し、オフピーク時にコンテンツエンジンに配布するようにスケジュールできます。

Cisco ACNSソフトウェアは、4つのDoS攻撃に対して脆弱で、管理者アカウントのデフォルトパスワードが含まれている可能性があります。ACNSソフトウェアを実行しているデバイスは、トランスペアレントプロキシサーバ、フォワードプロキシサーバ、またはリバースプロキシサーバとして設定されている場合、DoS攻撃に対して脆弱になる可能性があります。これらの問題の詳細は次を参照してください。

- **CSCef27476（登録ユーザ専用）：特別に巧妙に細工されたTransmission Control Protocol（TCP；伝送制御プロトコル）接続により、ACNSのキャッシュプロセスが再起動し、キャッシュされた情報が失われ、Webブラウザのコンテンツ要求のサービスが低下する可能性があります。**この脆弱性が繰り返し悪用されると、デバイスのキャッシュ機能に対する継続的なDoS攻撃が発生する可能性があります。
- **CSCef30460**：特定の不正なIPパケットにより、該当デバイスのCPU使用率が100 %に達し、すべてのサービスが低下する可能性があります。高いCPU使用率から回復するには、デバイスをリブートする必要があります。継続的な攻撃は結果的にサービス妨害攻撃（DoS）となります。
- **CSCeg49648**：特定の不正なパケットにより、RealServer RealSubscriberが該当デバイスのCPUの100 %を消費し、すべてのサービスが低下する可能性があります。高いCPU使用率から回復するには、デバイスをリブートする必要があります。継続的な攻撃は結果的にサービス妨害攻撃（DoS）となります。
- **CSCeg23731**：特定の巧妙に細工されたIPパケットにより、すべてのネットワーク帯域幅が消費され、ネットワーク使用率が100 %に達するまで、ACNSは細工されたパケットのコピーを継続的に転送する可能性があります。これにより、該当デバイスと同じローカルネットワークセグメント上にある該当デバイスおよびその他のデバイスに対するサービス拒否が発生する可能性があります。この状態から回復するには、デバイスをリブートする必要があります。この脆弱性が繰り返し悪用されると、ローカルネットワークセグメント上のすべてのデバイスに対して持続的なDoS攻撃が発生する可能性があります。
- **CSCef30743**：管理パスワードは、ACNS設定ダイアログが以前に実行されていない場合、または管理パスワードが手動で変更されていない場合は、すべてのインストールで同じデフォルトパスワードに設定されます。有効なサービスはすべて、デフォルトのクレデンシャルを使用します。

回避策

回避策の効果は、製品の組み合わせ、ネットワークトポロジ、トラフィックの動作、組織のミッションなど、お客様の状況によって異なります。該当する製品とリリースは多岐に渡るので、サービス プロバイダーやサポート機関に連絡し、ネットワーク内で使用するのに最も適した回避策を確認してから、実際に配備することを推奨いたします。

- Denial of Service(DoS)の脆弱性**CSCeg49648**に対して脆弱です。RealServer RealSubscriber（実行中の場合）。デフォルトでは、RealServer RealSubscriberは無効になっています。RealServer RealSubscriberを無効にすると、ACNSデバイスがRealServerストリーミングメディアキャッシュサブスクライバとして動作しなくなります。RealServer RealSubscriberが実行されているかどうかを確認するには、**show rtsp server real-subscriber**コマンドを使用します。次の出力は、有効なRealServer RealSubscriberを示しています。

```
cacheengine#show rtsp server

Real Subscriber version: ce7325-9.0.2.855
Real Subscriber enabled
Real Subscriber running
Real Subscriber end user license agreement accepted
Real Subscriber evaluation enabled. Estimated 17 days 21 hours left for evaluation.
Real Subscriber license key not installed
Real Subscriber bandwidth enforced is 522240 kbps
```

RealServer RealSubscriberを無効にするには、次に示すように、グローバルコンフィギュレーションモードでコマンド**no rtsp server real-subscriber enable**を使用します。

```
cacheengine#configure terminal
cacheengine(config)#no rtsp server real-subscriber enable
cacheengine(config)#exit
```

次の出力は、無効なRealServer RealSubscriberを示しています。

```
cacheengine#show rtsp server real-subscriber

Real Subscriber version: ce7325-9.0.2.855
Real Subscriber not enabled
Real Subscriber not running
Real Subscriber end user license agreement accepted
Real Subscriber evaluation enabled. Estimated 17 days 21 hours left for evaluation.
Real Subscriber license key not installed
Real Subscriber bandwidth enforced is 522240 kbps
```

RealServer RealSubscriberの実装の詳細については、『Cisco ACNSソフトウェア導入およびコンフィギュレーションガイド、リリース5.1』の「**RealSubscriberの有効化**」セクションを参照してください。
- 潜在的なデフォルトパスワードの問題**CSCef30743**に関しては、**setup dialog**が以前に実行されていたり、管理パスワードが以前に変更されていたりする場合、回避策は不要です。**setup**

dialogが実行されていない場合、または管理パスワードが変更されていない場合の回避策は、adminアカウントのパスワードを手動で変更することです。デフォルトのパスワードを変更するには、ユーザがadminユーザとしてログインした後にusernameコマンドを実行する必要があります。次に、コンソールポートを介して実行されるContent Engineのパスワード変更ダイアログの例を示します。

```
Username: admin
Password:
System Initialization Finished.
Cacheengine#configure terminal
cacheengine(config)#username admin password <password>
```

usernameコマンドの詳細については、次を参照してください。
Cisco ACNS 5.2ソフトウェアコマンドusernameCisco ACNS 5.1ソフトウェアコマンドusernameCisco ACNS 5.0ソフトウェアコマンドusernameCisco ACNS 4.2ソフトウェアコマンドusername

- サービス拒否(DoS)の脆弱性CSCef27476、CSCef30460、およびCSCeg23731に対しては、アクセスコントロールリスト(ACL)を使用して、これらの脆弱性の影響を減らすことができます。ACNSデバイス上およびスクリーニングルータ、スイッチ、ファイアウォール上にACLを設定し、ACNSデバイスへの内部および外部トラフィックをフィルタリングして、IPトラフィックが正当で信頼できるIPアドレスからのみ許可されるようにします。
スタンドアロンコンテンツエンジン用のIPアクセスコントロールリストの作成と管理については、http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/acns52/ldg52/acls.htmを参照してください。一元管理されたコンテンツエンジン用のIPアクセスコントロールリストの作成と管理については、http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/acns52/dcg52/5645acl.htmを参照してください。CiscoルータにACLを適用する方法の例については、http://www.cisco.com/warp/public/707/tacl.htmlを参照してください。アンチスプーフィングの詳細については、http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#sec_ipおよびhttp://www.ietf.org/rfc/rfc2827.txtを参照してください。ユニキャストリバースパス転送（ユニキャストRPF）機能は、スプーフィングされたIP送信元アドレスによって発生する問題を軽減するのに役立ちます。シスコのルータおよびファイアウォールで使用できます。詳細については、http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htmを参照してください。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/en/US/products/products_security_advisories_listing.htmlおよび後続のアドバイザリも参照して、問題の発生の可能性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。情報が明確でない場合は、Cisco Technical Assistance Center(TAC)に連絡して支援を求めてください。

DDTSバグID	脆弱性のあるACNSバージョン	修正済みバージョン
CSCef27476	リリース5.0.17.6より前の5.0	5.0.17.6 以降
	リリース5.1.11.6より前の5.1	5.1.11.6 以降
CSCef30460	すべての4.Xリリース	5.1.11.6以降にアップグレードする
	すべての5.0リリース	5.1.11.6以降にアップグレードする
	リリース5.1.11.6より前の5.1	5.1.11.6 以降
CSCeg49648	すべての5.1リリース	5.2.1.7以降にアップグレードする
CSCeg23731	すべての5.0リリース	5.1.13.7以降または5.2.3.9以降にアップグレードします。
	リリース5.1.13.7より前の5.1	5.1.13.7 以降
	リリース5.2.3.9より前の5.2	5.2.3.9 以降
CSCef30743	4.X、5.0、5.1、および5.2のすべてのリリース	アップグレードは不要です。必要に応じて、「回避策」セクションで説明されている回避策を実装します

アップグレード手順については、次のドキュメントを参照してください。

- **Cisco ACNSソフトウェアの導入および設定ガイド、リリース5.0**
  第10章：ソフトウェアのアップグレードとダウングレード
  注：この手順には、4.XソフトウェアからACNS 5.Xソフトウェアへの移行手順が含まれています
- **Cisco ACNSソフトウェアの導入および設定ガイド、リリース5.1**

第15章：ソフトウェアのアップグレードとダウングレード
注：この手順には、4.XソフトウェアからACNS 5.Xソフトウェアへの移行手順が含まれています

- **Cisco ACNS Software Configuration Guide for Centralized Managed Deployments、リリース5.2**
  第17章：ソフトウェアのアップグレードとダウングレード
  注：この手順には、4.XソフトウェアからACNS 5.Xソフトウェアへの移行手順が含まれています

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050224-acnsdos

改訂履歴

リビジョン 1.0	2005年2月24日	初回公開リリース

利用規約

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。