

Cisco Application Control Engine Administrator IP Address Overlap Vulnerability

Advisory ID: cisco-sa-20120620-ace

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ace>

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。

Revision 1.1

Last Updated 2012 June 20 19:27 UTC (GMT)

For Public Release 2012 June 20 16:00 UTC (GMT)

目次

- [要約](#)
- [該当製品](#)
- [詳細](#)
- [脆弱性スコア詳細](#)
- [影響](#)
- [ソフトウェア バージョンおよび修正](#)
- [回避策](#)
- [修正済みソフトウェアの入手](#)
- [不正利用事例と公式発表](#)
- [この通知のステータス : FINAL](#)
- [情報配信](#)
- [更新履歴](#)
- [シスコ セキュリティ手順](#)

要約

Cisco Application Control Engine (ACE) ソフトウェアには脆弱性が存在します。マルチコンテキスト モードで動作中、管理者権限のユーザが意図しないコンテキスト (仮想コンテキスト) にログインしてしまう可能性があります。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。この脆弱性には回避策があります。このアドバイザリは、次のリンク先で確認できます。

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ace>

該当製品

脆弱性が存在する製品

Cisco ACE アプライアンスまたはモジュールには、マルチコンテキスト モードでの動作中に脆弱性が存在します。この脆弱性を不正利用するには、2 つ以上のコンテキストが同じ管理 IP アドレスで設定されている必要があります。管理者が意図したコンテキストの管理 IP アドレスにアクセスを試みると、意図したものは別のコンテキストにログインしてしまう可能性があります。管理者が意図しないコンテキストの有効なログイン クレデンシャルを持っているとログインされ、持っていない場合はアクセスが拒否されます。

脆弱性が存在しない製品

他のシスコ製品において、この脆弱性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 アプライアンスまたはモジュールには、マルチコンテキスト モードでの動作中に脆弱性が存在します。この脆弱性を不正利用するには、2 つ以上のコンテキストが同じ管理 IP アドレスで設定されている必要があります。管理者が誤ったコンテキストの有効なログイン クレデンシャルを持っている場合は、そのコンテキストにログインされます。

この脆弱性は、Cisco Bug ID [CSCts30631](#) ([登録ユーザのみ](#)) として文書化され、Common Vulnerabilities and Exposures (CVE) ID として CVE-2012-3063 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System (CVSS) に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコは基本評価スコア (Base Score) および現状評価スコア (Temporal Score) を提供しています。お客様はこれらを用いて環境評価スコア (Environmental Score) を算出し、自身のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

<http://tools.cisco.com/security/center/cvssCalculator.x>

CSCts30631 - Block admin connections from overlapping contexts					
Calculate the environmental score of					
CVSS Base Score - 7.1					
Access	Access Comple	Authentica	Confidenti	Integrit	Availabi
s	Comple	tion	ality	y	lity

Vector	xity		Impact	Impact	Impact
Network	High	Single	Complete	Complete	Complete
CVSS Temporal Score - 5.9					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性が不正利用されると、ユーザは意図しないコンテキストに管理者としてログインしてしまう可能性があります。また、この状況は不注意で発生する場合があります。管理者は設定の閲覧や変更を行うことができます。

ソフトウェア バージョンおよび修正

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/go/psirt/> の Cisco Security Advisories and Responses アーカイブや、本アドバイザリ以降に公開のアドバイザリを参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

いずれの場合も、アップグレードするデバイス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。情報が不明確な場合は、Cisco Technical Assistance Center (TAC) もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

この脆弱性は、Cisco ACE ソフトウェア バージョン A4(2.3) および A5(1.1) ですすでに修正されています。ACE アプライアンスおよび ACE モジュール向けのこれらのソフトウェア バージョンは、Cisco Software Navigator から入手することができます。

<http://www.cisco.com/cisco/software/navigator.html>.

回避策

Cisco ACE のコンテキストごとに一意の管理 IP アドレスを設定します。設定リファレンスは次のリンクにあります。

http://www.cisco.com/en/US/partner/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA3_2_2/configuration/quick/guide/setup.html#wp1010576

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフ

トウェア ライセンスの条項に従うことに同意したことになります。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャンネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、[Cisco.com](http://www.cisco.com) の Software Navigator からアップグレードを入手することができます。<http://www.cisco.com/cisco/software/navigator.html>

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、適切な処置について支援を受けてください。

回避策の効果は、使用製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策または修正が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center (TAC) に連絡してアップグレードを入手してください。

- +1 800 553 2447 (北米内からのフリーダイヤル)
- +1 408 526 7209 (北米以外からの有料通話)
- 電子メール : tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このアドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC を通して無償アップグレードをお求めください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先を参照してください。

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team (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とその公表は確認しておりません。

この脆弱性は、お客様のケースへの対応中に発見されました。

この通知のステータス : FINAL

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を示唆するものでもありません。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

あるものとしします。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意識を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ace>

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

このアドバイザリに関する今後の更新があれば、Cisco.com に掲載されますが、メーリングリストで配信されるとは限りません。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.1	2012-June-20	Corrected CVE ID
Revision 1.0	2012-June-20	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報入手するための登録方法について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、<http://www.cisco.com/go/psirt/> で確認することができます。