Multiple Vulnerabilities in Cisco Secure Access Control System

Advisory ID: cisco-sa-20140115-csacs

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140115-csacs

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 1.0

For Public Release 2014 January 15 16:00 UTC (GMT)

目次

要約

Cisco Secure Access Control System（ACS）には、次の脆弱性が存在します。

- Cisco Secure ACS の RMI における権限昇格に関する脆弱性
- Cisco Secure ACS の RMI における認証されていないユーザのアクセスに関する脆弱性
- Cisco Secure ACS におけるオペレーティング システム コマンドの入力に関する脆弱性

Cisco Secure ACS は、TCP ポート 2020 および 2030 を使用したノード間通信に Remote Method Invocation（RMI）インターフェイスを使用します。

これらの脆弱性はそれぞれ独立しています。1 つの脆弱性に影響を受けるリリースが、その他の脆弱性からも影響を受けるとは限りません

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。このアドバイザリは、次のリンクで確認できます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140115-csacs

RMI に関連した脆弱性に対するネットワーク ベースの緩和策については、『Cisco Applied Mitigation Bulletin：Identifying and Mitigating the Multiple Vulnerabilities in Cisco Secure Access Control System』をご覧ください。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=32120

該当製品

脆弱性が認められる製品

リリース 5.5 より前の Cisco Secure ACS リリースはすべて、このアドバイザリに記載されている RMI 関連の脆弱性の影響を受けます。

リリース 5.4 パッチ 3 より前の Cisco Secure ACS リリースはすべて、このアドバイザリに記載されている OS コマンド入力に関する脆弱性の影響を受けます。

脆弱性が認められない製品

次の Cisco Secure Access Control Server 製品はこの脆弱性の影響を受けません。

- Cisco Secure Access Control Server for Windows
- Cisco Secure Access Control Server Express
- Cisco Secure Access Control Server View
- Cisco Secure Access Control Server Solution Engine

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 TrustSec ソリューションの主要コンポーネントの 1 つである Cisco Secure ACS は、RADIUS および TACACS+ サービスを提供する高度なポリシー プラットフォームです。アクセス コントロールの管理とコンプライアンスに関する新たな要求に対応するためには、これまで以上に複雑なポリシーが必要であり、Cisco Secure ACS を使用すればこのようなポリシーに対応できます。Cisco Secure ACS により、デバイス管理や、無線/有線 802.1x、およびリモート VPN でのネットワーク アクセスを目的としたアクセス ポリシーの集中管理が可能になります。アイデンティティ ストアは内部または外部のどちらを利用することも可能です。内部アイデンティティ ストアには、内部 データベース内に保存されているユーザ クレデンシャル情報が入っています。Cisco Secure ACS は、外部アイデンティティ ストアを通じて、外部データベースから情報を取得します。

Cisco Secure ACS の RMI における権限昇格に関する脆弱性

Cisco Secure ACS の RMI インターフェイスに関する脆弱性により、認証されたリモートの攻撃者が superadmin としてアクションを実行できる可能性があります。

この脆弱性は、許可が適切に適用されないことに起因します。攻撃者は、認証されているユーザ アカウントを使用し、RMI を通じて ACS にアクセスすることで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は RMI を通じて superadmin の機能を実行できるようになります。

この脆弱性は、Cisco Bug ID CSCud75180（ 登録ユーザ専用 ）として文書化され、CVE ID CVE-2014-0649 が割り当てられています。

Cisco Secure ACS の RMI における認証されていないユーザのアクセスに関する脆弱性

Cisco Secure Access Control System（ACS）の RMI インターフェイスの脆弱性により、認証されていないリモートの攻撃者が RMI インターフェイスを通じて ACS にアクセスできる可能性があります。

この脆弱性は、認証と許可が適切に適用されないことに起因します。攻撃者は、RMI インターフェイスを通じて ACS にアクセスすることで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は ACS にアクセスし、管理アクションを実行できる可能性があります。

この脆弱性は、Cisco Bug ID CSCud75187（ 登録ユーザ専用 ）として文書化され、CVE ID CVE-2014-0648 が割り当てられています。

RMI インターフェイスは、TCP ポート 2020 および TCP ポート 2030 を使用してデータを伝送します。RMI インターフェイスは、分散導入環境における Cisco ACS ノード間の通信に使用されます。

Cisco Secure ACS におけるオペレーティング システム コマンドの入力に関する脆弱性

Cisco Secure ACS の Web インターフェイスの脆弱性により、認証されたリモートの攻撃者がオペレーティング システム レベルのコマンドを入力できる可能性があります。

この脆弱性は、入力が適切に検証されないことに起因します。攻撃者は、ACS Web インターフェイスの特定の場所にオペレーティング システム コマンドを入力することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はシェル アクセス権を持たずにオペレーティング システム レベルのコマンドを実行し、システムの機密性、完全性、または可用性に影響を及ぼす可能性があります。

この脆弱性は、Cisco Bug ID CSCue65962（ 登録ユーザ専用 ）として文書化され、CVE ID CVE-2014-0650 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。本セキュリティ 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。

シスコでは、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知ることができます。

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

またシスコでは、各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/

CSCud75180- RMI Privilege Escalation Vulnerability Calculate the environmental score of					
CVSS Base Score - **8.5**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	Single	Complete	Complete	Complete
CVSS Temporal Score - **7.0**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCud75187- Unauthenticated Access to RMI Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.6**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	None	Complete	Complete	Complete
CVSS Temporal Score - **6.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCue65962- ACS GUI Arbitrary OS Command Injection Vulnerability Calculate the environmental score of					
CVSS Base Score - **8.5**					
Access	Access Comple	Authentication	Confidentiality	Integrity	Availability

Vector	xity		Impact	Impact	Impact
Network	Medium	Single	Complete	Complete	Complete
CVSS Temporal Score - **7.0**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

Cisco Secure ACS の RMI における権限昇格に関する脆弱性の不正利用に成功すると、権限を持たず認証されている攻撃者が、RMI インターフェイスを通じて該当システムにアクセスする権限を得る可能性があります。

Cisco Secure ACS の RMI における認証されていないユーザのアクセスに関する脆弱性の不正利用に成功すると、認証されていない攻撃者が、RMI インターフェイスを通じて該当システムにアクセスする権限を得る可能性があります。

Cisco Secure ACS におけるオペレーティング システム コマンドの入力に関する脆弱性の不正利用に成功すると、認証されていない攻撃者が、ACS の Web インターフェイスからオペレーティング システム レベルのコマンドを実行する可能性があります。

ソフトウェア バージョンおよび修正

以下の表に、影響を受ける Cisco Secure ACS の最初の修正リリースの情報を記載します。この表の最後の列が、本アドバイザリに記載されているすべての脆弱性に対する修正が含まれたリリース バージョンです。

	5.0	5.1	5.2	5.3	
Cisco Secure ACS RMI Privilege Escalation Vulernability	Migrate to 5.5 or later	Migrate to 5.5 or later	Migrate to 5.5 or later	Migrate to 5.5 or later	Mi to
Cisco Secure ACS RMI Unauthenticated User Access Vulnerability	Migrate to 5.5 or later	Migrate to 5.5 or later	Migrate to 5.5 or later	Migrate to 5.5 or later	Mi to
Cisco Secure ACS Operating System Command Injection Vulnerability	Migrate to 5.4 or later	Migrate to 5.4 or later	Migrate to 5.4 or later	Migrate to 5.4 or later	5.4 Pa
First Fixed release for all vulnerabilities in this advisory					**5.5**

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, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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デバイスに十分なメモリがあること、現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、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。

Cisco Secure ACS 5.5 は、Cisco.com の Software Center (

http://www.cisco.com/cisco/software/navigator.html ）にアクセスし、 **[Products] > [Security] > [Access Control and Policy] > [Policy and Access Management] > [Cisco Secure Access Control System] > [Cisco Secure Access Control System 5.5]** の順に選択してダウンロードできます。

回避策

これらの脆弱性に対する設定上の回避策はありません。

RMI に関連した脆弱性に対するネットワークベースの緩和策については、『Cisco Applied Mitigation Bulletin:

Identifying and Mitigating the Multiple Vulnerabilities in Cisco Secure Access Control System』 をご覧ください。

http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=32120

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ーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

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ーチャ 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 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、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、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に関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象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ことを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したものの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

たは、サードパーティ ベンダーから購入したものの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 ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの 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 に無償アップグレードをリクエストしてください。

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（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

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。

これらの脆弱性は、シスコの社内テストで発見されたものです。

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ます。またシスコ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訳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-20140115-csacs

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 E 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

本アドバイザリに関する今後の更新は 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。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2014-January-15	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サポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。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。