Cisco Secure Access Control System SQL Injection Vulnerability

Advisory ID: cisco-sa-20150211-csacs

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150211-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 2015 February 11 16:00 UTC (GMT)

目次

要約

バージョン 5.5 パッチ 7 より前の Cisco Secure Access Control System（ACS）では、ACS View レポート インターフェイス ページにおける SQL インジェクション攻撃に対する脆弱があります。この不正利用に成功した場合、認証されたリモートの攻撃者は、ACS View データベースの 1 つに保存されている RADIUS アカウンティング レコードなどの情報へのアクセスや変更、または基盤となるファイル システム内の情報へのアクセスが可能となる場合があります。

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-20150211-csacs

該当製品

脆弱性が認められる製品

バージョン 5.5 パッチ 7 より前の Cisco Secure ACS バージョンはすべて、このアドバイザリに記載されている SQL インジェクションの脆弱性の影響を受けます。

脆弱性が認められない製品

Cisco Secure ACS バージョン 5.6 以降は、この脆弱性の影響を受けません。

次の Cisco Secure ACS 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 ACS の Web フレームワーク コードに存在する脆弱性により、認証されたリモートの攻撃者によって 2 つの ACS View データベースのうちの 1 つで任意の SQL クエリが実行される可能性があります。認証には ACS 管理者アカウントへのアクセスが必要です。

この脆弱性は、レポート アプリケーションに渡される、ユーザから提供された入力を適切にサニタイズできないことに起因します。攻撃者は、HTTP プロトコルを使用して、巧妙に細工されたリクエストを Web サーバに送信することで、この脆弱性を不正利用します。

この脆弱性は、Cisco Bug ID CSCuq79027（登録ユーザ専用）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2015-0580 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、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

CSCuq79027 - Cisco Secure Access Control Server SQL injection Calculate the environmental score of					
CVSS Base Score - **9.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - **7.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

認証されたリモートの攻撃者は、この脆弱性を不正利用することで、アクティブなユーザ セッションを追跡するために使用する Cisco ACS View データベースからレコードにアクセスできる可能性があります。攻撃に成功すると、RADIUS アカウンティング レコードから機密データを取得したり、機密データを変更できる場合があります。また攻撃者は、 基盤のオペレーティング システムから情報にアクセスできる可能性があります。

ただし、この脆弱性によってメインの ACS データベースからユーザ アカウント情報を変更または直接消去することはできません。

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, 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。

回避策

この脆弱性に対処する既知の回避策はありません。

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。

この脆弱性は、ING Services Polska 社の Lukasz Plonka 氏よりご報告いただきました。

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 に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150211-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
- fulldisclosure@seclists.org

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。

今後のドキュメントや関連コンテンツの入手手順については、Security Vulnerability Policy ページの Receiving Security Vulnerability Information from Cisco を参照してください。

更新履歴

Revision 1.0	2015-February-11	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、Cisco Security Advisory 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 Cisco Security Advisory は、http://www.cisco.com/go/psirt/ で確認することができます。