Cisco ATA 187 Analog Telephone Adaptor Remote Access Vulnerability

Advisory ID: cisco-sa-20130206-ata187

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130206-ata187/

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 2013 February 6 16:00 UTC (GMT)

目次

要約

Cisco ATA 187 Analog Telephone Adaptor のファームウェア バージョン 9.2.1.0 および 9.2.3.1 には、認証されていないリモートの攻撃者による、該当デバイスのオペレーティング システムへのアクセスを許可する可能性のある脆弱性が存在します。

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。 これらの脆弱性に対して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-20130206-ata187/

該当製品

脆弱性が存在する製品

Cisco ATA 187 Analog Telephone Adaptor は、ファームウェア バージョン 9.2.1.0 または 9.2.3.1 を稼働している場合、この脆弱性の影響を受けます。

Cisco ATA 187 Analog Telephone Adaptor のファームウェア バージョンは、管理者がデバイスの Web インターフェイスで **SW_Version ID** フィールドを表示して確認することができます。

脆弱性が存在しない製品

次のシスコ製品には、脆弱性は存在しません。

- Cisco ATA 186 Analog Telephone Adaptor
- Cisco ATA 188 Analog Telephone Adaptor

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 ATA 187 Analog Telephone Adaptor のファームウェア バージョン 9.2.1.0 および 9.2.3.1 には、認証されていないリモートの攻撃者による、該当デバイスのオペレーティング システムへのアクセスを許可する可能性のある脆弱性が存在します。

この脆弱性は、TCP ポート 7870 での認証に対する不適切な検証と、オペレーティング システム内でのコマンドに対する不適切な許可に起因します。該当するシステムに攻撃者が接続し、任意のコマンドを送信することで、この脆弱性を不正利用する可能性があります。
この脆弱性は、Cisco Bug ID CSCtz67038 (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-2013-1111 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/

CSCtz67038: Cisco ATA 187 Analog Telephone Adaptor Remote Access Vulnerability

Calculate the environmental score of					
CVSS Base Score - **9.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	Partial	Complete
CVSS Temporal Score - **7.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

注： このアドバイザリでは 1 つの脆弱性として示していますが、本来の CVSS の定義によると、実際には 2 つの脆弱性が含まれています。第一の脆弱性は、デバイスのアクセス コントロール回避です。第二の脆弱性は、デバイスでの認証されていないコマンドの実行です。これら連鎖型の脆弱性の重大度を適切に表すため、ここでは 1 つの脆弱性として扱っています。

影響

この脆弱性の不正利用に成功した場合、サービス拒否（DoS）状態が引き起こされたり、デバイス上でオペレーティング システムのコマンドが実行されたり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

この脆弱性は、Cisco ATA 187 Analog Telephone Adaptor ファームウェア バージョン 9.2.3.1 ES ビルド 4 以降で修正されています。

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、後続のアドバイザリを参照して、起こりうる障害とそれに対応できるアップグレード 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。

現在、Cisco.com の Cisco Software ダウンロード セクションに Cisco ATA 187 Analog Telephone Adaptor ファームウェアのリリースを追加公開する予定はありません。

修正済みのリリースが必要なお客様は、このアドバイザリの「修正済みソフトウェアの入手」セクションに記載したサポート組織にお問い合わせください。

回避策

デバイスにリモートからアクセスして、プロセスをリストアップし、Telnet プロセスを終了させ

ることで、デバイスの Telnet プロセスを終了することができます。これにより、デバイスがリロードされない限り、デバイスへのリモート アクセスを防ぐことができます。

ネットワーク内のシスコ デバイスに適用可能なその他の緩和策については、次のリンクにあるこのアドバイザリの付属ドキュメント『Identifying and Mitigating Exploitation of the Cisco ATA 187 Analog Telephone Adaptor Remote Access Vulnerability』にて参照できます。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=27921

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。

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、E 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、カスタマー サポート リクエストの処理中に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-20130206-ata187/

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

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 1.0	2013-February-06	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を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。