Cisco IOS認証要求処理におけるDoS脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20120823-CVE-2012-1338 **初公開日 :** 2012-08-23 18:12 **バージョン 1.0 :** Final **CVSSスコア :** 4.9 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2012-1338

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 IOSには、認証されたリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性のある脆弱性が存在します。

この脆弱性は、Web認証要求の不適切な処理に起因します。認証されたリモート攻撃者は、該当ソフトウェアに悪意のある認証要求を送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、DoS状態が発生する可能性があります。

シスコはこの脆弱性を確認し、ソフトウェアアップデートをリリースしました。

この脆弱性を不正利用するには、認証が必要であり、攻撃者はターゲットデバイスに隣接するネットワークへのアクセスを必要とする可能性があります。これらの要件により、悪用の難易度が高まります。

該当製品

シスコは、Cisco Bug ID CSCts88664のリリースノートを次のリンクでリリースしました。 Cisco IOS 15.0SE

脆弱性のある製品

Cisco Catalyst 3750-EおよびCisco Catalyst 3560-Eシリーズスイッチ上のCisco IOSリリース15.0SE、15.0SG、および15.0EWには脆弱性が存在します。

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。

回避策

適切なアップデートを適用することを推奨します。

IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけに該当システムへのアクセスを許可することを検討することもできます。

重要なシステムを監視することを推奨します。

修正済みソフトウェア

有効な契約を結んでいるシスコのお客様は、 CiscoのSoftware Centerからアップデートを入手できます。契約を結んでいないシスコのお客様は、Cisco Technical Assistance Center(TAC)に1-800-553-2447または1-408-526-7209で連絡するか、次のEメールでアップグレードを入手できます。 *tac@cisco.com にアクセスしてください。*

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20120823-CVE-2012-1338

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2012年8月23日

利用規約

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も示唆するものではありません。 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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。