Cisco IOSソフトウェア SSH バナー プロセスエラー サービス拒否の脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20110824-CVE-2011-1624 **初公開日 :** 2011-08-24 14:19 **バージョン 1.0 :** Final **CVSSスコア :** 6.8 **回避策 :** Yes **Cisco バグ ID :**	CVE-2011-1624

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ソフトウェアにより認証される可能にする可能性があるサービス拒否（DoS）状態を引き起こすために脆弱性がリモート攻撃者含まれています。

脆弱性は Cisco IOSソフトウェアによってログイン バナーの不適当な処理が原因です。 認証されて 2 セッションを使用して SSH によってログオンによって、リモート攻撃者この脆弱性を不正利用する可能性があります。 成功すれば、攻撃者によりデバイスは DoS 状態に終って、リロードします可能性があります。

Cisco はソフトウェア リリース メモの脆弱性を確認し、更新済ソフトウェアをリリースしました。

脆弱性を不正利用するために、攻撃者は目標とされたデバイスに SSH によってログインにできる必要があります。 アクセス 要件は影響を受けたシステムの現在のユーザにエクスプロイトの出典を制限します。 エクスプロイトは正規のユーザが 2 SSH セッションを使用してログインに試みるとき偶然起こるかもしれません。

該当製品

修正済みソフトウェア

Cisco IOS ソフトウェア バージョン 12.2(58)SE は脆弱です。

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。

改訂履歴

バージョン	説明	Section	ステータス	日付
1.0	初版リリース	該当なし	Final	2011-Aug-24

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。