Cisco IOS XR ソフトウェア SSH サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20100120-xr-ssh
初公開日 : 2010-01-20 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : Yes
Cisco バグ ID :

CVE-2010-0137

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 XR ソフトウェアの SSH サーバ実装はサービス拒否状態を引き起こすのに不正利用する非認証が、リモートユーザ可能性がある脆弱性が含まれています。

攻撃者は新しい SSH 接続ハンドラにプロセスがクラッシュしますかもしれない巧妙に細工された SSH バージョン 2 パケットの送信によってこの脆弱性を引き起こす可能性があります。 繰り返された利用により各々の新しい SSH 接続ハンドラにプロセスは消費される他のシステム の 機能性に逆効果をもたらすかもしれない不安定な状態をもたらす可能性があるかなりのメモリにクラッシュし、導きますかもしれません。 このイベントの間に、親 SSH デーモン プロセスは普通機能し続けます。

シスコはこの脆弱性に対処するソフトウェア アップデートをリリースしました。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100120-xr-ssh で掲示されます。

該当製品

修正済みソフトウェア

この脆弱性は Cisco IOS XR ソフトウェアの影響を受けたバージョンを稼動して、有効に なる SSH サーバ 機能がある Cisco IOS XR システムに影響を及ぼします。 有効に なった SSH サーバ 機能とのシステムに設定で現在のコマンド **ssh サーバ [v2] が**あります。 Cisco IOS XR ソフトウェアの SSH サーバの設定に関する追加詳細については

http://www.cisco.com/en/US/docs/routers/crs/software/crs_r3.9/security/configuration/guide/sc39ssh.html#wp1044523 で「Cisco IOS XR システム セキュリティ コンフィギュレーション ガイド」を参照して下さい。

SSH サーバは Cisco IOS XR ソフトウェアで「セキュリティ」パッケージ情報 エンベロープ（円）がインストールされている場合しか有効に することができません。 管理者はセキュリティ パイがインストールされているかどうか確認する**提示インストール summary コマンドを**発行できます。 このコマンドはセキュリティ円がインストールされている場合 "<platform>-k9sec-<version>" か、たとえば、"c12k-k9sec-3.6.1" と同じようなアクティブなパッケージを表示するものです。

仕様によって影響を受けるソフトウェア バージョンの情報に関してはこのアドバイザリの「ソフトウェア バージョン および 修正」セクションを参照して下さい。

脆弱性を含んでいないことが確認された製品

Cisco IOSソフトウェアの SSH サーバ実装および Cisco IOS XE ソフトウェアはこの脆弱性から影響を受けません。

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

リビジョン 1.0	2010-January-20	初版リリース

利用規約