

Cisco Service Control エンジン サービス拒否の脆弱性

High	アドバイザーID : cisco-sa-20080521-sce	CVE-2008-0536
	初公開日 : 2008-05-21 16:00	0536
	バージョン 1.0 : Final	CVE-2008-0534
	CVSSスコア : 7.8	0534
	回避策 : Yes	CVE-2008-0535
	Cisco バグ ID :	0535

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

3 セキュア シェル (SSH) 脆弱性は SCE のシステム不安定な状態からリロードという結果に終るかもしれない Cisco Service Control エンジン (SCE) にあります。最初の脆弱性は積極的な時間枠の内で行なわれる SSH ログオン アクティビティの間に引き起こされるかもしれませんが。2つめの脆弱性は同時に発生する他の SCE 管理操作と組み合わせて標準 SSH ログオン アクティビティと引き起こされるかもしれませんが。第3脆弱性は SSH ログオンの間に引き起こされるかもしれ、ユニークで無効な認証クレデンシャルの使用方法に特定です。

Cisco は影響を受けた顧客向けのこれらの脆弱性に対処するために無償アップグレード ソフトウェアを使用できるようにしました。これらの脆弱性に対する回避策はありません。

注: これらの脆弱性は、互いに独立して存在します。デバイスは 1 脆弱性のない他から影響を受けるかもしれません。

このアドバイザーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080521-sce> で掲示されます。

該当製品

修正済みソフトウェア

SCE 1000 および 2000 シリーズ デバイスは次の脆弱性から SCE の SSH サーバが有効になる場合影響を受けます:

- SSH ログオン アクティビティへのシステム脆弱性- 3.1.6 以前の影響 SCE ソフトウェアバージョン。
- SSH ログオン アクティビティは 3.0.7 および 3.1.0 前に不正な 入出力 オペレーションの影響 SCE ソフトウェア バージョン原因となります。
- SCE SSH 認証 シーケンス異常- 3.1.6 以前の影響 SCE ソフトウェア バージョン。

注: SCE SSH サーバはデフォルトでディセーブルにされます。

Cisco Service Control オペレーティング システム (SCOS) ソフトウェアの脆弱なバージョンを実行しているかどうか判別するために、「Show version」 Command Line Interface (CLI) コマンドを発行して下さい。次の例はソフトウェア リリース 3.1.6 を実行する Cisco SCE を示したものです:

```
SCE2000#>show version
System version: Version 3.1.6 Build 157
Build time: Mar 31 2008, 18:58:49 (Change-list 303626)
Software version is: Version 3.1.6 Build 157
```

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

リビジョン 1.0	2008-May-21	初回公開リリース
--------------	-------------	----------

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、単独の転載や意識を施した場合、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。