OpenSSH サーバ の 脆弱性

severity	**アドバイザリーID :** cisco-sa-20030917-openssh **初公開日 :** 2003-09-17 07:00 **バージョン 1.6 :** Final **回避策 :** Yes **Cisco バグ ID :**	CVE-2003-0695 CVE-2003-0682 CVE-2003-0693

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

SSH サーバのための OpenSSH 実装の新しい脆弱性は発表されました。

OpenSSH 実装に基づいて SSH サーバを実行する影響を受けたネットワークデバイスはエクスプロイト スクリプトが同じデバイスに対して繰り返し実行されるときサービス拒絶 （ DoS ） 攻撃に脆弱かもしれません。 これらの脆弱性に対しては、影響を緩和するための回避策があります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030917-openssh で掲示されます。

該当製品

修正済みソフトウェア

以下の製品に、OpenSSH コードに基づいて SSH サーバ実装があり OpenSSH 脆弱性から影響を受けます。

- Cisco Catalyst スイッチング ソフトウェア（ CatOS ）
  Cisco のさまざまな Catalystファミリースイッチは CatOS ベース リリースか IOSベース の リリースを実行します。
  IOSベース の リリースは脆弱ではないです。
  6.x、7.x および 8.x リリース トレインのすべての K9 （ 暗号 ）イメージはこれらの脆弱性から影響を受けます。 それらに SSH サポートがないので CatOS リリース 2.x、3.x、4.x および 5.x は脆弱ではないです。

Cisco 次の Catalyst スイッチは脆弱です:
- Catalyst 6000 シリーズ
- Catalyst 5000 シリーズ
- Catalyst 4000 シリーズ
- Catalyst 2948G、2980G、2980G-A、4912G - Catalyst 4000 シリーズ コード ベースを使用して下さい
ソフトウェアリビジョンを確認するために、コマンド・ライン プロンプトで **show version コマンドを**タイプして下さい。

- Cisco Secure Intrusion Detection System（NetRanger）アプライアンス
次のデバイスは（ソフトウェア バージョン 3.0(1) ～ 4.1(1) を実行する）脆弱です:
- IDS-42xx アプライアンス
- NM-CIDS
- WS-SVS-IDSM2
- Cisco Catalyst 6000 および 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのための Ciscoネットワーク 分析 モジュール（NAM）
K9 暗号パッチを加え、有効に なる SSH がある次のデバイスは脆弱です:
- WS-X6380-NAM、ソフトウェア バージョン 2.1(2) または 3.1(1a) を実行します
- WS-SVC-NAM-1、ソフトウェア バージョン 2.2(1a) または 3.1(1a) を実行します
- WS-SVC-NAM-2、ソフトウェア バージョン 2.2(1a) または 3.1(1a) を実行します
- CiscoWorks 1105 Hosting Solution Engine（HSE）
- CiscoWorks 1105 Wireless LAN Solution Engine（WLSE）
- Cisco コンテンツサービス CSS 11000 スイッチ シリーズ
- Ciscoアプリケーション及び Content Networking Software（ACNS）
- BTS 10200 Softswitch
- Cisco GSS 4480 Global Site Selector
- Cisco SN 5428 ストレージ ルータ
- Cisco PGW 2200 ソフトスイッチ（以前 Cisco VSC 3000 と Cisco SC 2200 として知られている）

Cisco は SN5420 ストレージ ルータのための SSH のコードをリリースしませんでした。

脆弱性を含んでいないことが確認された製品

SSH サーバを織込んでいる以下の製品は OpenSSH 脆弱性に**脆弱**であるために確認されました。

- Cisco IOS、SSH 両方バージョン 1.5 および SSH バージョン 2.0
- Cisco Secure Intrusion Detection System Catalystモジュール（IDSM）—型番 WS-X6381-IDS
- Cisco PIX ファイアウォール
- Cisco Catalyst 6000 FireWall Service Module（FWSM）
- Cisco VPN 3000 コンセントレータおよび Cisco VPN 5000 コンセントレータ
- Cisco MDS 9000 Series Multilayer Switches

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

Revision 1.6	2003-November-07	脆弱なプロダクトとして追加された Cisco PGW 2200 ソフトスイッチ。 CatOS のための修正済みリリースとして追加された 8.1(3)。
Revision 1.5	2003-September-27	詳細 セクションの OpenSSH 携帯用バージョンへの追加された脆弱。 脆弱追加された ACNS および BTS10200。 CSS11000 のための影響を受けされたリリースとして追加された 5.x。 NAM のための更新済修正情報。
リビジョン 1.4	2003-September-23	ソフトウェア バージョン および 修正 の追加された CatOS リリース スケジュール。
リビジョン 1.3	2003-September-19	影響を受けていますとして追加された Cisco コンテンツサービス CSS11000 スイッチ シリーズおよび Ciscoネットワーク 分析 モジュール（NAM）。
リビジョン 1.2	2003-September-18	Workaround セクションの CatOS のための追加回避策を追加しました。
リビジョン 1.1	2003-September-18	Affected Products セクションへの追加された CatOS バージョン、Cisco Secure Intrusion Detection System（NetRanger）アプライアンスおよび Cisco GSS 4480 グローバルサイトセレクタ; そして脆弱 で はないリストへの Cisco Secure Intrusion Detection System Catalystモジュール（IDSM）。 製品のための詳細 セクションおよび追加されたバグID への追加された Cisco Secure Intrusion Detection System（NetRanger）アプライアンスおよび Cisco GSS 4480 グローバルサイトセレクタ。 ソフトウェア バージョン および 修正 セクションへの追加された Cisco Secure Intrusion Detection System（NetRanger）アプライアンス、および製品のための追加された次の修正。
リビジョン 1.0	2003-September-17	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。