IOS HTTP 認証の脆弱性

severity	**アドバイザリーID :** cisco-sa-20010627-ios-http-level	CVE-2001-0537
	初公開日 : 2001-06-27 15:00	
	バージョン 1.8 : Final	
	回避策 : Yes	
	Cisco バグ ID :	

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

HTTPサーバが有効に なり、ローカル許可は使用されるとき認証をバイパスし、デバイスのコマンドを実行するために、可能性のある、ある状況下では、です。 そのケースでは、ユーザはデバイスを完全な制御をコントロールできます。 すべてのコマンドは最も高い特権（15）レベルと実行されます。

Cisco IOSÂ® ソフトウェアのすべてのリリースは、リリース 11.3 およびそれ以降にはじまって、脆弱です。 Cisco IOSソフトウェアを実行する事実上すべての主流 Ciscoルータおよびスイッチはこの脆弱性から影響を受けます。

Cisco IOSソフトウェアを実行していない製品は脆弱ではないです。

この脆弱性のための回避策はルータ ディセーブルにすることまたは（TACACS+）または Radius の HTTPサーバを認証のために Terminal Access Controller Access Control System（TACACS+）使用することです。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010627-ios-http-level で掲示されます。

該当製品

修正済みソフトウェア

Cisco IOS ソフトウェア Release 11.3 と それ以降を実行するどのデバイスでも脆弱です。

該当する Cisco IOS ソフトウェア リリースと動作するかもしれない Ciscoデバイスはに含んでいますが、制限されません:

- AGS/MGS/CGS/AGS+、IGS、RSM、800、ubr900、1000、1400、1500、1600、1700、2500、2600、3000、3600、3800、4000、4500、4700、AS5200、AS5300、AS5800、6400、7000、7100、7200、ubr7200、7500、および 12000 シリーズの Ciscoルータ。
- LS1010 ATM スイッチのほとんどの最近のバージョン。
- それらが Cisco IOSソフトウェアを実行する場合 Catalyst 6000 および 5000。
- Cisco IOSソフトウェアを実行するときだけ Catalyst 2900XL および 3500XL LAN スイッチ。
- Catalyst 2900 および 3000 シリーズ LANスイッチは影響を受けています。
- Cisco Distributed Director。

いくつかの製品に関しては、該当するソフトウェア リリースは比較的新しく、上記リストに記載されている各デバイスで利用可能ではないかもしれません。

脆弱性を含んでいないことが確認された製品

Cisco IOSソフトウェアを実行しない場合、この脆弱性から影響を受けません。

Cisco IOSソフトウェアを実行しないし、この問題から含んでいる影響を受けないシスコ製品は、に制限されませんが:

- 700 シリーズ ダイヤル式ルータ（750、760、および 770 シリーズ）。
- Catalyst 6000 および 5000 はそれらが Cisco IOSソフトウェアを実行しない場合影響を受けていません。
- IGX および BPX 行の WANスイッチングプロダクト。
- MGX（以前 AXISシェルフとして知られている）。
- ホストベース ソフトウェア。
- Cisco PIX Firewall。
- Cisco Local Director。
- Cisco Cache Engine。

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 1.8	2003-Sep-23	不正利用事例と公式発表 セクションの更新済第 2 段落
Revision 1.7	2001-Sep-13	中間からの最終への更新済ステータス。
Revision 1.6	2001-Sep-10	更新済回避策 セクション。
Revision 1.5	2001-Aug-08	Catalyst 3500 XL が含まれる更新済該当製品
リビジョン 1.4	2001-July-19	修正された該当製品、IOS 表および回避策セクション。

リビジョン 1.3	2001-July-13	更新済回避策 セクション; Affected Products セクションからの削除された Catalyst 1900 および 2800。
リビジョン 1.2	2001-June-29	更新済プラットフォーム記述
リビジョン 1.1	2001-June-28	更新済ソフトウェアが利用可能な日付
リビジョン 1.0	2001-June-27	初版リリース

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。