Cisco IOS HTTP サーバのクエリに関する脆弱性

severity

アドバイザリーID : cisco-sa-20001025-ios-http-server-query

初公開日 : 2000-10-25 16:00

バージョン 1.6 : 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

Cisco IOSソフトウェアの複数のリリースの問題により Ciscoルータを引き起こしますまたは IOS HTTP サービスが有効に なれば切り替えることは参照する停止し、リロードするために、「http://router-ip/anytext?/ に」試みられ、要求されたときイネーブルパスワードは供給されます。この問題がサービス拒絶（DoS）攻撃を生成 するのに利用することができます。

Cisco バグ ID **CSCdr91706** として識別される脆弱性は Cisco IOS ソフトウェア リリース 12.0 ～ 12.1 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に含んだ影響を与えます。 これは **CSCdr36952** と同じ問題ではないです。

脆弱性は解決され、Cisco は修正済みリソースをすべての該当する IOS リリースを無料交換できるようにしています。 下記の詳細に示すようにこの問題に脆弱ではない顧客はリリースにアップグレードするように勧められます。

この脆弱性はイネーブルパスワードが知られている設定 されなければときだけ不正利用することができます。

完全なアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20001025-ios-http-server-query で利用できます。

該当製品

修正済みソフトウェア

以下の製品は問題がある Cisco IOS ソフトウェア リリースを実行する場合影響を受けています。 Cisco製品がデバイスに影響を受けた IOS を、ログイン確認し実行した、コマンド **show version** を発行するためかどうか。 Cisco IOSソフトウェアは「**インターネットワーク オペレ**

ーティング システム ソフトウェア」または「IOS（tm）」ソフトウェアとしてそれ自身を識別し、ディスプレイをバージョン番号。 他の Ciscoデバイスにコマンド **show version** がありませんし、異なる出力を与えません。 ルータから得られるソフトウェア バージョン および 修正 下記の例で示されるバージョンとバージョン番号を比較して下さい。

該当する IOSソフトウェアリリースと動作するかもしれない Ciscoデバイスは下記のものを含んでいます:

- 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、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。
- IOS を実行する場合 Catalyst 6000。
- IOS を実行するときだけ Catalyst 2900XL LAN スイッチ。
- Catalyst 1900、2800、2900、3000、および 5000 シリーズ LANスイッチ影響を受けていて下さい。
- Cisco DistributedDirector。

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 ダイヤルアップルータ（750、760、および 770 シリーズ）は影響を受けていません。
- Catalyst 6000 は IOS 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は影響を受けていません。
- MGX は（以前 AXISシェルフとして知られている）影響を受けていません。
- Cisco PIX Firewall は影響を受けていません。
- Cisco LocalDirector は影響を受けていません。
- Cisco Cache Engine は影響を受けていません。

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

Revision 1.6	2006-March-17	「ソフトウェア バージョン および 修正」セクションの 12.1XC への変更された 12.XC; 更新済 FINALステータス テキスト。

Revision 1.5	2003-March-05	追加された追加バグID は他の影響を受けたハードウェアのために詳しく区分します。
リビジョン 1.4	2002-September-25	最終への更新済この通知 の ステータス セクション。
リビジョン 1.3	2000-November-01	「Catalyst 1900、2800、2900、3000、の更新済 Affected Products セクションはおよび 5000 シリーズ LANスイッチ影響を受けています」。 変化しない 11.2 リリースのリストからの取除かれた "11.2 SA」。 前に 12.0 ベースの該当するリリースへの追加された "11.2 SA」。 12.0T のための追加された有効 日付およびアップグレード バージョン。 変更された文は「選択し、設定しますネットワークデバイスの強力なパスワードを」。「選択し、設定して下さいネットワークデバイスの強いイネーブルパスワードを」。
リビジョン 1.2	2000-October-26	12.1 XF、12.1 XG および 12.1 XP のための更新済表ヒント。 追加された Catalyst 2800 ように「該当製品」セクションの影響を受けた製品。
リビジョン 1.1	2000-October-25	12.1T および 12.1AA のための更新済表ヒント。
リビジョン 1.0	2000-October-25	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。