Cisco IOS BGP 属性破損の脆弱性

severity

アドバイザリーID : cisco-sa-20010510-ios-bgp-attr

初公開日 : 2001-05-10 15:00

バージョン 1.1 : 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

ボーダー ゲートウェイ プロトコル（BGP）アップデートは宛先にパスを記述する属性およびネットワーク レイヤ到着可能性情報（NLRI）が含まれています。 認識されない通過型属性により認識されない通過型属性をクリアする試みにより遅い失敗まで認識されない通過型属性を受取り次第クラッシュから、及ぶ Cisco IOS ルータで失敗を引き起こす場合があります。 仕様しかし一般的 な 設定は影響を受け、下記です。 失敗は他のベンダーの BGP 実装の機能不全が理由で検出されました。 回避策はありません。 影響を受けた顧客は修正されたコード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 Cisco バグ ID CSCdt79947 を割り当てられました。

このアドバイザリの完全 な テキストは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010510-ios-bgp-attr にあります

該当製品

修正済みソフトウェア

受信ルート ルート・ マップとフィルタリングする BGP4 プレフィクスを含むコンフィギュレーションは脆弱です。 プレフィクス 受信 routemap フィルタリングの BGP は Cisco IOSÂ® ソフトウェア バージョン 11.2 Cisco IOSソフトウェアの次のバージョンが下記の表でで影響を受け、リストされている導入されました: 11.CC および派生物、11.2 および derivaties、12.0 から奪取 される 11.3、11.3T、12.0、12.0S および特別なブランチは影響を受けるすべてです。 12.1 に、12.0(5)T 基づく、Cisco IOSソフトウェアのバージョン 12.2、12.0ST、および 12.1(E) は影響を受けていません。 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、**show version コマンドを**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**show version コマンドが**ありませんし、別の出力を与えません。 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 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。

脆弱性を含んでいないことが確認された製品

従って Cisco IOSソフトウェアを実行するかもしれない Ciscoデバイスは BGP をサポートしないし、脆弱下記のものを含んでいますです:

- 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。
- Cisco DistributedDirector。

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。 BGP 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。
- ホストベース ソフトウェアは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

リビジョ	2001-Novembe	いくつかの IOSバージョンに関する推奨事項をアップグレードする行われた

ン 1.1	r-29	変更を
リビジョン 1.0	2001- May-10	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。