Cisco IOS ARPテーブルオーバーライト の 脆弱性

severity	**アドバイザリーID :** cisco-sa-20011115-ios-arp-overwrite	CVE-2001-0895
	初公開日 : 2001-11-15 16:00	
	バージョン 1.3 : 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

ルータを引き起こす可能性があるか、または Cisco IOSÂ® ソフトウェア リリースの特定のバージョンをローカルルータの ARPパケットを送信 し、受信することを止めるように実行することを切り替えるためにインターフェイスさせなさいローカルブロードキャスト インターフェイスのアドレス解決プロトコル（ARP）パケットを送信 することは可能性のあるです（たとえば、イーサネット、ケーブル、トークン リング、FDDI）。 これは近いうちにルータおよびローカル ホストをパケットを互いに送信することが引き起こします。 ARPパケットはルータの自身のインターフェイス アドレスのためのルータによって受け取りましたが、別のメディア アクセス制御（MAC）アドレスは受信された ARPパケットからのものの ARPテーブルのルータの MAC アドレスを上書きします。 これは Black Hat 会議の出席者に公知 の 事項であると示され、考慮する必要があります。 この攻撃は攻撃者か攻撃ホストにセグメント ローカルのデバイスに対してだけ正常です。

この脆弱性は Cisco バグ ID CSCdu81936 で文書化されています、回避策は利用できます。

完全な表記は http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20011115-ios-arp-overwrite 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
- Catalyst 2900XL および 3500XL LAN スイッチ
- Catalyst 2950 LAN スイッチ
- Catalyst 3550 スイッチ
- Catalyst 2948G-L3 及び 4908G-L3
- Catalyst 4000 レイヤ3 サービス モジュール（WS-X4232-L3）
- Catalyst 5000 RSM/RSFC
- Catalyst 6000 MSFC
- Native IOS を実行する Catalyst 6000
- Catalyst 8500 MSR/CSR
- Cisco DistributedDirector

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。
- 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。
- CatOS が稼働している Catalyst 2901/2902、2948G、2980G、4000、5000、および 6000 のスイッチ。

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 1.3	2002-July-22	ソフトウェア バージョン および 修正 セクションへの更新。
リビジョン 1.2	2001-December-18	要約、該当製品、影響、ソフトウェア バージョン および 修正 および回避策セクションへの更新。
リビジョン 1.1	2001-November-21	テーブルアップデートをリリースして下さい
リビジョン 1.0	2001-November-15	に関しては一般公開 15-NOV-2001 08:00 AM US/Pacific（UTC-0700）

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。