Cisco IOS 以外 の 製品のための形式の異なる SNMP メッセージ処理の脆弱性

severity	**アドバイザリーID :** cisco-sa-20020211-snmp-msgs-non-ios	CVE-2002-0012
	初公開日 : 2002-02-11 23:00	CVE-2002-0013
	バージョン 2.6 : 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

複数のシスコ製品は簡易ネットワーク管理プロトコル（SNMP）メッセージの処理で脆弱性が含まれています。 これらの脆弱性がサービス拒否を生成 するのに繰り返し不正利用することができます。 ほとんどの場合、回避策は影響を軽減するかもしれないこと利用できます。 いくつかのこれらの脆弱性は VU#617947、VU#107186、OUSPG #0100、CAN-2002-0012 および CAN-2002-0013 としてさまざまなグループ識別されます。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020211-snmp-msgs-non-ios で利用でき、Cisco IOSソフトウェアを実行しないシスコ製品に適用すると同時にこの脆弱性を記述します。

ドキュメントガイドは Cisco IOSソフトウェアを実行する製品のためのこの脆弱性を、http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml 記述します。

該当製品

修正済みソフトウェア

製品に脆弱性があるかどうかについては、以下のリストを確認してください。 ソフトウェアバージョンまたは設定情報が示されている場合は、その組み合せにのみ脆弱性があります。

- Catalyst 290x、292x、2948g、3000、3200、3900、4000、4912g、5000 シリーズ スイッチ
- Catalyst 6000 Supervisor モジュール、Catalyst 6000 Network Analysis Module（NAM）
- MicroHub 1500,MicroSwitch 1538/1548

- BPX、IGX、MGX WAN スイッチおよびサービス拡張シェルフ
- WAN Manager
- Cisco Secure PIX Firewall
- （Microsoft SNMP が有効に なれば ） CallManager
- （Microsoft SNMP が有効に なれば ）ユニティサーバ
- Cisco Secure Intrusion Detection System（NetRanger ）アプライアンスおよび IDS モジュール
- BR340、WGB340、AP340、AP350、BR350 Cisco/Aironet無線 製品
- CSS11000（Arrowpoint ） Content Services Switch
- Content Engine 507、560、590、および 7320 実行 3.1、4.0.1、か 4.0.3
- コンテンツルータ 4430 およびコンテンツ 配信 マネージャ 4630 および 4650 実行 4.0
- LocalDirector
- Internet CDN Content Engine 590 および 7320、コンテンツディストリビューションマネージャ 4670、およびコンテンツルータ 4450 実行 ICDNソフトウェア 1.0、2.0、2.1.0
- VPN3000（Altiga ） VPN コンセントレータ
- アクセス レジストラ（Solaris SNMP を使用して ）
- Cisco ws-x6608 および ws-x6624 IP テレフォニー モジュール
- トラフィックディレクター
- Cisco Info Center
- Switch Probe
- CiscoWorks Windows
- Hosting Solution Engine
- ユーザ登録ツール VLAN方針 サーバ
- Cisco Element Management Framework
- Cisco Intelligent Contact Management
- Cisco ONS 15454 optical transport platform
- Cisco ONS 15327 メトロエッジオプティカルトランスポートプラットフォーム
- VG248 Analog Phone Gateway
- Cisco 8110 ブロードバンド ネットワーク終端ユニット
- Cisco FastHub 400

脆弱性を含んでいないことが確認された製品

以下のシスコ製品はこの脆弱性から脆弱ではないか、または SNMP をサポートしないので影響を受けません。 ソフトウェア バージョンか構成情報が提供される場合、それらの組み合わせだけ脆弱ではないです。

- Catalyst 1900 ， 2820 シリーズ スイッチ
- Catalyst 1400 FDDI コンセントレータ
- FastHub 300 Ethernet リピータ
- Cache Engine 505 および 570 実行バージョン 2.3 または 2.5
- Content Engine 507、560 および 590 の実行バージョン 2.3 または 2.5
- Content Engine 507 および 560、コンテンツルータ 4430 およびコンテンツ 配信 マネージ

ャ 4630 および 4650 実行 E-CDN 3.0.x
- コンテンツ ルータ ソフトウェアを実行する CR-4430-B
- IP/TV
- Device Fault Manager
- ME1100 シリーズ
- Voice Manager
- RTM
- IP Phone（ すべてのモデル ）
- SN5400 シリーズ ストレージ ルータ
- VPN5000 VPN コンセントレータ
- Cisco ONS 15190/15194 IP Transport コンセントレータ
- Cisco ONS 15800/15801/15808 Dense Wave Division Multiplexing プラットフォーム
- Cisco ONS 15830 T30 光増幅システム
- Cisco ONS 15531/15532 T31 OMDS メトロ WDMシステム
- Cisco ONS 15831/15832 T31 DWDM システム
- Cisco ONS 15863 T31 Submarine WDM システム

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 2.6	2004-Mar-01	ソフトウェア バージョン および 修正表 Voice Products セクションに行われる更新。
Revision 2.5	2003-Jan-24	ソフトウェア バージョン および 修正に行われた更新は最終にステータス変更しました。
Revision 2.4	2002-Apr-02	ソフトウェア バージョン および 修正に行われる更新。
Revision 2.3	2002-Apr-01	該当製品に行われる更新およびソフトウェア バージョン および 修正。
Revision 2.2	2002-Mar-13	該当製品に行われる更新。
Revision 2.1	2002-Mar-08	該当製品に行われる更新およびソフトウェア バージョン および 修正。
Revision 2.0	2002-Feb-25	今 IOS 以外 の 製品 ソフトウェア バージョン および 修正への別途のアドバイザリ、更新、および回避策。
リビジョン 1.3	2002-Feb-20	以降のセクションに行われる更新: ソフトウェア バージョン および 修正および回避策- LocalDirector
リビジョン 1.2	2002-Feb-16	以降のセクションに行われる更新: 要約、ソフトウェア バージョン および 修正、回避策
リビジョン 1.1	2002-Feb-13	テーブルアップデート

リビジョン 1.0	2002-Feb-12	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。