SNMP メッセージ処理の脆弱性

severity

アドバイザリーID : cisco-sa-20040420-snmp

初公開日 : 2004-04-20 21:00

バージョン 1.5 : Final

回避策 : Yes

Cisco バグ ID : CSCed68575

CVE-2004-0714

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インターネットワーク オペレーティング システム（IOS）ソフトウェア リリース トレイン 12.0S、12.1E、12.2、12.2S、12.3、12.3B および 12.3T は場合不正利用されたデバイスがリロードします可能性がある SNMP 要求の処理で脆弱性が含まれているかもしれません。

脆弱性はある特定の IOS リリース ルータおよびスイッチにだけ on Cisco あります。 この動作はコード変更によってもたらされ、CSCed68575 と解決されます。

この脆弱性はリモートで 引き起こすことができます。 この脆弱性の不正利用の成功によりデバイスのリロードを引き起こすかもしれ、サービス拒否 （DoS）を生成 するのに繰り返し不正利用できます。

このアドバイザリは 420-snmp で利用できます。

該当製品

修正済みソフトウェア

この脆弱性は CSCeb22276 のためのコード変更によってもたらされました。 この変更は脆弱にこれらのリリースをする次のリリースに保存されました。

Cisco IOSソフトウェアを実行する Cisco Catalyst ATM モジュールは影響を受けていません。

ONS 15454（40-DMX）-C Band-Even Channels Transmission Module 15454E は、ML シリーズ ラインカードおよび実行リリース 4.60 で設定されたとき脆弱であり。 ONS 15454（40-DMX）-C Band-Even Channels Transmission Module 15454E ソフトウェアは ML シリーズ ラインカードで動作する Cisco IOSソフトウェアの脆弱なバージョンを組み込み。 該当するリリ

ースを実行する ML シリーズ ラインカードのないコンフィギュレーションは脆弱ではないです。 リリース 4.60 は脆弱である 12.1(20)EO を組み込みます。

次の CCO によって掲示されるリリースは SNMP 問題に脆弱であると知られています。 Cisco で最もよいナレッジに、他の掲示されたリリースは影響を受けていません。 しかし Cisco はあらゆる更新の場合にこのリストを修正するかもしれません。 Cisco によって送達された暫時かカスタム リリースはまた脆弱かもしれません。 暫定ビルドに関する詳細については、http://www.cisco.com/warp/public/620/1.html のセクション 3.6 を参照して下さい。

完全な Cisco IOS ソフトウェア アップグレード 表についてはこのアドバイザリのソフトウェア バージョン および 修正 セクションを参照して下さい。

- 12.0(23)S4
- 12.0(23)S5
- 12.0(24)S4
- 12.0(24)S4a
- 12.0(24)S5
- 12.0(26)S1
- 12.0(27)S
- 12.0(27)SV
- 12.0(27)SV1
- 12.1(20)E
- 12.1(20)E1
- 12.1(20)E2
- 12.1(20)EA1
- 12.1(20)EB
- 12.1(20)EC
- 12.1(20)EC1
- 12.1(20)EO
- 12.1(20)EU
- 12.1(20)EW
- 12.1(20)EW1
- 12.2(12g)
- 12.2(12h)M1
- 12.2(12h)
- 12.2(20)S
- 12.2(20)S1
- 12.2(20)SW
- 12.2(21)
- 12.2(21a)
- 12.2(21)SW
- 12.2(21)ZQ
- 12.2(23)

- 12.3(2)XC1
- 12.3(2)XC2
- 12.3(2)XE
- 12.3(2)XF
- 12.3(4)T
- 12.3(4)T1
- 12.3(4)T2
- 12.3(4)T2a
- 12.3(4)T3
- 12.3(4)XD
- 12.3(4)XD1
- 12.3(4)XG
- 12.3(5)
- 12.3(5a)B
- 12.3(5a)
- 12.3(5b)
- 12.3(6)

Cisco 製品で稼働しているソフトウェアを確認するには、デバイスにログインし、**show version** コマンドを発行してシステム バナーを表示します。 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」としてそれ自身をまたは単に「IOSÂ®」識別します。 出力次の行で、イメージ名は「バージョンに」先行しているかっこIOSリリース名の間で表示する。 その他の Cisco デバイスには **show version** コマンドがないか、異なる出力が返されます。

次の例は C2500-IS-L のインストール済みイメージ名前と IOS リリース 12.0(3) を実行するCisco製品を指定したものです:

```
Cisco Internetwork Operating System Software IOS (TM)

2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

リリース トレイン ラベルは "12.0" です。

次 の 例は C2600-JS-MZ のイメージ名と IOS リリース 12.0(2a)T1 を実行する製品を示します:

```
Cisco Internetwork Operating System Software IOS (tm)

C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

Cisco IOS リリース指名についてのその他の情報は http://www.cisco.com/warp/public/620/1.html で見つけることができます。

脆弱性を含んでいないことが確認された製品

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 1.5	2004-May-05	12.0S、12.1EB、12.2、12.2S、12.2SW、12.3、12.3T、12.3XH、12.3XK および 12.3XQ のための情報更新済ソフトウェア アベイラビリティの。 追加される新しいリリース無し。
リビジョン 1.4	2004-April-29	12.3XC のためのエントリ修正されるソフトウェア バージョン および 修正 セクションでは。
リビジョン 1.3	2004-April-23	別々のラインの各リリース リストされている Affected Products セクションでは。
リビジョン 1.2	2004-April-23	リリースの Affected Products セクション、修飾された第 4 段落およびアップデートされたリスト。 ソフトウェア バージョン および 修正では、12.1EB のための修正された/追加記入、12.1EO、12.1EU、12.2SW、12.2ZQ、12.2XE、12.2XF 区分して下さい
リビジョン 1.1	2004-April-22	ソフトウェア バージョン および 修正 セクション、追加された Optical製品 表およびアップデートされた IOS リリース 表。 Affected Products セクションでは、追加された Catalyst および Optical製品および 12.1(20)EO。
リビジョン 1.0	2004-April-20	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。