Cisco IOS ソフトウェアの SNMP Read-Write ILMI コミュニティ ストリングの脆弱性

severity

アドバイザリーID : cisco-sa-20010227-ios-snmp-ilmi

初公開日 : 2001-02-27 09:00

バージョン 1.5 : 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

バージョン 11.x および 12.0 に基づく Cisco IOSÂ® ソフトウェア リリースは SNMP オブジェクトの限られた数が文書化されていない ILMIコミュニティストリングを使用して許可なしで表示され、修正されるようにする欠陥が含まれています。 デバイスの正常な動作に影響を与えない場合予想に反して修正された混合を引き起こすかもしれないいくつかの変更可能なオブジェクトは「sysContact」のような MIB-IIシステムグループに、「sysLocation」、および「sysName」制限されます。 残りのオブジェクトは LANエミュレーション クライアントおよび PNNI MIB で含まれ、それらのオブジェクトの修正は ATM 設定に影響を与えるかもしれません。 影響を受けたデバイスは ILMIコミュニティストリングの不正使用から保護されない場合サービス拒否攻撃に脆弱であるかもしれません。

脆弱性は IOS リリース ルータおよびスイッチのある特定の組み合わせにだけ on Cisco あります。 ILMI は ATM のための必要なコンポーネントであり、脆弱性は ATM接続をサポートするATMインターフェイスの実際の存在かデバイスの物理的 な 能力に関係なく ATM および ILMI のための支援ソフトウェアが含まれている各 IOS リリースにあります。

この脆弱性を取除くために、Cisco はすべての影響を受けたプラットフォームのための無償ソフトウェアアップグレードを提供しています。 問題は DDTS レコード CSCdp11863 で文書化されています。

ソフトウェアアップグレードの代りに、回避策はある特定の IOS リリースに ILMIコミュニティまたは「**ilmi**」意見をディセーブルにし、SNMP に不正アクセスを防ぐためにアクセス リストを追加することによって適用することができます。 どの影響を受けたシステムでも、ソフトウェア リリースに関係なくネットワーク 境界のまたは個々のデバイスの SNMP トラフィックのフィルタリングによって、保護することができます。

この表記は http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010227-ios-snmp-ilmi で掲示されます。

該当製品

修正済みソフトウェア

脆弱性はルータおよびスイッチ製品のために非同期転送モード（ATM）ネットワーキングおよび暫定ローカル管理インターフェイス（ILMI）のためのサポートが含まれている、ATMインターフェイスをサポートするために物理的 な機能に関係なくあります Cisco IOS ソフトウェア バージョン 11.x および 12.0 のある特定のリリースにだけあり。

10.3 およびそれ以前に基づく Cisco IOS ソフトウェア バージョンは脆弱性が含まれていません。 問題は 11.0(0.2) でもたらされました。 12.1 およびそれ以降のすべての Cisco IOS ソフトウェア リリースはこのアドバイザリに説明がある問題に脆弱修理され、ではないです。

デバイスに Cisco製品、ログインで動作するソフトウェアを判別し、システムバナーを表示するためにコマンド「**show version**」を発行するため。 Cisco IOSソフトウェアは「　」としてそれ自身をまたは単に「`IOS tm`」識別します。 イメージ名は「バージョン」および IOSリリース名に先行している出力次の行のかっこの間で、通常表示する。 他の Ciscoデバイスに" show version " コマンドがありませんまたはために別の出力を与えて下さい。

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
```

該当する IOSソフトウェアリリースを実行するかもしれない Ciscoデバイスは含んでいますが、に制限されません:

- Cisco 1400 および 1700 シリーズ。
- Cisco 2600（但し例外としては c2600-c-mz、c2600-d-mz、c2600-i-mz、c2600-io3-mz および c2600-ix-mz イメージ脆弱 でであってはなりません）。
- Catalyst 2900 ATM、2900XL および 2948g シリーズ。
- Cisco 3620（但し例外としては c3620-d-mz、c3620-i-mz、c3620-io3-mz および c3620-ix-mz イメージ脆弱 でであってはなりません）。
- Cisco 3640（但し例外としては c3640-d-mz、c3640-i-mz、c3640-io3-mz および c3640-ix-mz イメージ脆弱 でであってはなりません）。
- Cisco 3660（但し例外としては c3660-d-mz、c3660-i-mz および c3660-ix-mz イメージ脆弱 でであってはなりません）。
- Cisco MC3810（但し例外としては mc3810-i-mz、mc3810-is-mz、mc3810-is56i-mz および mc3810-js-mz イメージ脆弱 でであってはなりません）。
- Catalyst 4232、4840g、5000 の RSFC シリーズ スイッチ。

- Cisco 4500，4700 および 5800 DSC シリーズ。
- Cisco 6200、6400 NRP および 6400 NSP シリーズ。
- Catalyst MSM（c6msm）、6000 Hybrid Mode（c6msfc）、および 6000 Native Mode（c6sup）。
- Cisco RSM、7000、7010、7100、7200、ubr7200 および 7500 シリーズ。
- Catalyst 8510CSR、8510MSR、8540CSR および 8540MSR シリーズ。
- Cisco 10000 ESR および 12000 GSR シリーズ。
- LS1010 および Cisco 6260-NI2。
- DistributedDirector（但し例外としては igs-w3 イメージ脆弱 でであってはなりません）。

脆弱性を含んでいないことが確認された製品

ATM および ILMI のためのサポートがないのでこの脆弱性から影響を受けないシスコ製品は、IOS を実行しないのでまたは含んで下さい、しかしに制限されません:

- Catalyst ATM Blade（実行可能性のある影響を受けたコードは、しかしブレードへの SNMP 接続可能性のあるではないです）。
- Cisco 800 および 805 シリーズ。
- Cisco ユニバーサル ブロードバンドルータ ubr900 および ubr920。
- Cisco 1003，1004 および 1005 シリーズ。
- Cisco 1600、2500、2800、4000 シリーズ。
- Cisco 2500 固定 Frad。
- Cisco 3800（MC3810 と混同されないため）。
- Cisco 5100，5200 および 5300 シリーズ アクセス サーバ。
- Catalyst 6000 Supervisor モジュール。
- Cisco PIX Firewall。
- Aironet および Cisco/Aironet無線 製品。
- CS11000、Cache Engine、LocalDirector およびネットワーク スケーリング製品（但し例外としては Distributed Director 影響を受けるかもしれません）。
- Altiga コンセントレータのような VPN 製品。
- ホストベースの ネットワーク管理かアクセス 管理 プロダクト。
- Cisco IP Telephony およびテレフォニー管理用ソフト（脆弱 な IOSプラットフォームでホストされる）それらを除いて。
- 音声ゲートウェイおよび統合 プラットフォーム（脆弱 な IOSプラットフォームでホストされる）それらを除いて。
- ONS 15000 シリーズのような光スイッチ プロダクト。

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	2001-March-07	表の訂正された修正済みリリースバージョン

リビジョン 1.4	2001-March-02	表の訂正された修正済みリリースバージョン
リビジョン 1.3	2001-February-28	表の訂正された修正済みリリースバージョン、修正された回避策明確にするために
リビジョン 1.2	2001-February-27	該当製品で訂正されるエラー
リビジョン 1.1	2001-February-27	回避策で訂正されるエラー
リビジョン 1.0	2001-February-27	最初臨時 パブリック バージョン

利用規約