Cisco IOS ソフトウェア SNMP 読み取り/書き込み ILMI コミュニティ文字列の脆弱性

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 : No Workarounds available
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 IOS®ソフトウェアリリースには、許可がなくても、ドキュメント化されていないILMIコミュニティストリングを使用して限定された数のSNMPオブジェクトを表示および変更できる不具合が含まれています。一部の変更可能なオブジェクトは、「sysContact」、「sysLocation」、「sysName」などのMIB-IIシステムグループに制限されています。これらはデバイスの通常の動作には影響しませんが、予期せず変更されると混乱を引き起こす可能性があります。残りのオブジェクトはLAN-EMULATION-CLIENTおよびPNNI MIBに含まれており、これらのオブジェクトの変更はATM設定に影響を与える可能性があります。該当するデバイスがILMIコミュニティストリングの不正使用から保護されていない場合、サービス拒否攻撃に対して脆弱になる可能性があります。

この脆弱性は、Ciscoルータおよびスイッチの IOSリリースの特定の組み合わせにのみ存在します。ILMIはATMに必要なコンポーネントであり、この脆弱性は、ATMインターフェイスの実際の存在やATM接続をサポートするデバイスの物理的な機能とは無関係に、ATMとILMIをサポートするソフトウェアが含まれているIOSリリースごとに存在します。

この脆弱性を排除するため、シスコでは該当するすべてのプラットフォームに対して無償のソフトウェアアップグレードを提供しています。この不具合は、DDTSレコードCSCdp11863で文書化されています。

ソフトウェアのアップグレードの代わりに、ILMIコミュニティまたは「*ilmi」ビューを無効にし、アクセスリストを適用してSNMPへの不正アクセスを防止することで、特定のIOSリリースに回避策を適用できます。影響を受けるシステムは、ソフトウェアリリースに関係なく、ネットワーク境界または個々のデバイスでSNMPトラフィックをフィルタリングすることで保護できます。

この通知はhttps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010227-ios-snmp-ilmiで公開されます。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

この脆弱性は、Asynchronous Transfer Mode（ATM；非同期転送モード）ネットワーキングおよびInterim Local Management Interface（ILMI；暫定ローカル管理インターフェイス）のサポートを含むルータおよびスイッチ製品用のCisco IOSソフトウェアバージョン11.xおよび12.0の特定のリリースにのみ存在し、ATMインターフェイスをサポートする物理的な機能には関係ありません。

10.3以前のバージョンのCisco IOSソフトウェアには、この脆弱性は含まれていません。この不具合は11.0(0.2)で導入されました。12.1以降のすべてのCisco IOSソフトウェアリリースは修復されており、このアドバイザリに記載されている不具合に対する脆弱性はありません。

シスコ製品で実行され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てコマンド「show version」を発行し、システムバナーを表示します。Cisco IOSソフトウェアは、「Internetwork Operating System Software」または単に「IOS(tm)」と表示されます。イメージ名は括弧の間に表示されます。通常は出力の次の行に表示され、その後に「バージョン」とIOSリリース名が続きます。他のシスコデバイスには「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、IOSリリース12.0(3)が稼働し、インストールされているイメージ名がC2500-IS-Lであるシスコ製品を示しています。

```
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が稼働しているシスコデバイスには次のものが含まれますが、これらに限定されるものではありません。

- Cisco 1400 および 1700 シリーズ.
- Cisco 2600（c2600-c-mz、c2600-d-mz、c2600-i-mz、c2600-io3-mz、およびc2600-ix-mzイメージには脆弱性はありません）。
- Catalyst 2900 ATM、2900XL、2948gシリーズ。
- Cisco 3620（ただし、c3620-d-mz、c3620-i-mz、c3620-io3-mz、およびc3620-ix-mzイメージには脆弱性はありません）。

- Cisco 3640（ただし、c3640-d-mz、c3640-i-mz、c3640-io3-mz、およびc3640-ix-mzイメージには脆弱性はありません）。
- Cisco 3660（ただし、c3660-d-mz、c3660-i-mz、およびc3660-ix-mzイメージには脆弱性はありません）。
- Cisco MC3810（ただし、mc3810-i-mz、mc3810-is-mz、mc3810-is56i-mz、およびmc3810-js-mzイメージには脆弱性はありません）。
- Catalyst 4232、4840g、5000 RSFCシリーズスイッチ
- Cisco 4500、4700、5800 DSCシリーズ
- Cisco 6200、6400 NRP、6400 NSPシリーズ
- Catalyst MSM(c6msm)、6000ハイブリッドモード(c6msfc)、および6000ネイティブモード(c6sup)
- Cisco RSM、7000、7010、7100、7200、ubr7200、および7500シリーズ
- Catalyst 8510CSR、8510MSR、8540CSR、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（ただし、igs-w3イメージには脆弱性はありません）。

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をサポートしていない、またはIOSを実行していないなどの理由で、この脆弱性の影響を受けないシスコ製品には次のものが含まれますが、これらに限定されません。

- Catalyst ATMブレード（該当する可能性のあるコードは実行されますが、ブレードへのSNMP接続は不可能です）
- 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、1005シリーズ
- Cisco 1600、2500、2800、4000シリーズ
- Cisco 2500固定Frad
- Cisco 3800（MC3810と混同しないこと）
- Cisco 5100、5200、5300シリーズアクセスサーバ
- Catalyst 6000スーパーバイザモジュール。
- Cisco PIX ファイアウォール.
- AironetおよびCisco/Aironetワイヤレス製品。
- CS11000、Cache Engine、LocalDirector、およびネットワークスケーリング製品（Distributed Directorが影響を受ける可能性がある場合を除く）
- Altigaコンセントレータなどの VPN製品
- ホストベースのネットワーク管理製品またはアクセス管理製品。
- Cisco IP Telephonyおよびテレフォニー管理ソフトウェア（脆弱性のあるIOSプラットフォームでホストされているソフトウェアを除く）
- 音声ゲートウェイおよびコンバージェンスプラットフォーム（脆弱性のあるIOSプラットフォームでホストされているものを除く）

- ONS 15000シリーズなどの光スイッチ製品。

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。

詳細

ILMI(Interim Local Management Interface)は、ATM（非同期転送モード）インターフェイスの設定に使用される独立した業界標準です。この規格では、SNMP(Simple Network Management Protocol)で以前に定義されたメカニズムと形式の使用が規定されています。ILMI通信はSNMPに基づいていますが、実際には、物理ATMリンクのみを通過するIP（インターネットプロトコル）以外のトランスポートを使用して行われます。ILMIは、ATM自動検出やLANE（LANエミュレーション）などの機能に不可欠です。

SNMPの「オブジェクト」は、MIB(Management Information Base)に編成された変数です。MIBはツリー構造になっており、動作（読み取り専用）データと設定（読み取り/書き込み）オプションの両方が含まれています。SNMP要求で「ILMI」というコミュニティストリングを指定することにより、MIB-IIシステムグループ、LAN-EMULATION-CLIENT MIB、およびPNNI(Private Network-to-Network Interface)MIBという、この脆弱性の影響を受けるデバイスの全体的な管理ツリー構造の3つの特定部分にあるオブジェクトを読み取るためのアクセス権を取得できます。各パーツ内のオブジェクトのサブセットは、同じ「ILMI」コミュニティストリングを使用して変更できます。

MIB-IIシステムグループには、デバイス自体に関する基本情報が含まれています。変更可能なオブジェクトの数は制限されています。次に例を示します。

- system.sysContact：デバイスの管理を担当する個人または組織の連絡先情報。
- system.sysLocation：デバイスがインストールまたは動作している物理的な場所の説明。
- system.sysName：デバイスのホスト名、およびコンソールプロンプトでそれ自体を識別する方法。（これは、ネットワーク上の他のホストがデバイスを認識するときに使用する名前とは異なる場合があります）。

システムMIBのほとんどのオブジェクトは読み取り専用であり、SNMPでは変更できません。たとえば、前回の再起動からの経過時間、デバイスのハードウェアおよびソフトウェアのテキストによる説明などです。

LAN-EMULATION-CLIENT MIBおよびPNNI MIBでは多数のオブジェクトを表示できます。また、一部の読み取り/書き込みオブジェクトの変更は、デバイスのATM動作に影響を与える可能性があります。LAN-EMULATION-CLIENT MIBのオブジェクトは、LANEがすでにデバイスに設定されている場合にのみ表示または変更できます。

Cisco IOSソフトウェアでのSNMPへのアクセスは、アクセスコントロールリスト(ACL)の適用、SNMPビューの変更または削除、実行コンフィギュレーションからのコミュニティストリングの削除、またはSNMPサービスの無効化によって制限できます。アクセスの基準を満たさないSNMPクエリは、このような保護手段が講じられた時点で速やかに廃棄されます。クエリがアク

セスの基準を満たさない場合、応答が作成されて送信されます。

すべてのIOS 11.1以降のリリースでILMIコミュニティストリングを使用できないようにデバイスを設定できます。これを実現するために選択される特定の方法は、特定のIOSリリースと設定によって異なります。

この不具合は、CSCdp11863で文書化されています。この脆弱性は、「ILMI」コミュニティストリングを使用するSNMP要求がILMIによって転送された場合にのみ認識されるようにテストを実施することで修正されます。

ATM機能は、Cisco IOSソフトウェアのさまざまな10.xリリースで追加されました。ただし、不具合を含む機能は、ILMIおよびその他のATM機能のサポートがIOSリリース11.0(0.2)で追加されたときに導入されました。したがって、以前のリリースには脆弱性はありません。

追加のSNMP脆弱性に関しては、別途Cisco Security Advisoryが発表されています。この通知と並行して、このアドバイザリhttp://www.cisco.com/warp/public/707/ios-snmp-community-vulns-pub.shtmlも参照してください。

回避策

お客様のニーズ、機器、およびソフトウェアの機能に基づいて、いくつかの回避策があります。各回避策の有用性と実用性は、デバイスで実行されているIOSリリースと、お客様の環境の多くの変数によって異なります。導入する前に、次の各選択肢を慎重に検討することをお勧めします。これらの回避策が必要になるのは、該当しないリリースのIOSソフトウェアにアップグレードできない場合だけです。

1. 他の回避策が有効でないリリースで使用するデフォルトの回避策：
    a. すべてのホストからのSNMPをブロックしている脆弱なデバイスのすべてのインターフェイスにアクセスリストを適用する（デバイスを管理する権限を持つホスト以外）。
    b. 望ましくないSNMPトラフィックが脆弱性のあるデバイスを含むネットワークに入るのを防ぐために、ネットワークのエッジでSNMPアクセスをブロックする。

   アクセスリストは、ネットワークの動作とパフォーマンスに与える可能性のある影響を慎重に考慮して導入する必要があります。また、IP送信元アドレスに基づく認証は脆弱であるため、前述の方法では、IP送信元アドレスがスプーフィングされている特定の種類の攻撃から保護できないことに注意してください。詳細については、http://www.cisco.com/warp/public/707/21.htmlにあるシスコのドキュメント『Improving Security on Cisco Routers』を参照してください。
2. IOS 11.1に基づく該当リリース：
    a. ビューを削除して、ILMIコミュニティに到達できないようにします。
    snmp-server view *ilmiなし
    b. この設定は、システムのリロード後も有効になりません。このコマンドは、システムを再起動するたびに再入力する必要があります。

3. 該当するIOS 11.2 ~ 11.3(8)のリリースでATMを必要としない場合：
   この影響を受けるリリースの範囲では、ILMIコミュニティストリングを変更または削除できます。ただし、デバイスをリブートしても変更内容は保持されません。これらの手順は、該当デバイスのシステムをリロードするたびに再適用する必要があります。
   a. ドキュメントに記載されていないILMIコミュニティストリングを公開し、変更できるようにします。
      snmpサーバコミュニティILMI RW
      上記のコマンドを実行すると、エラーが発生する場合がありますが、無視しても問題はありません。
   b. 同じコミュニティの読み取り/書き込み機能を無効にします。
      no snmp-server community ILMI RWコマンド
      エラーが表示された場合は、この回避策をデバイスに適用できません。上記の最初の項目に示されているデフォルトの回避策を使用します。
   c. この設定はシステムのリロード後も有効ではないため、システムを再起動するたびにコマンドを再入力する必要があります。
   上記の項目2のコマンドでエラーが発生せず、このデバイスでATMが必要ない場合は、この回避策は完了です。
4. ATMを必要とするIOS 11.2 ~ 11.3(8)の該当リリースについては、次の手順を実行します。

   注：この回避策は、LS1010や8500シリーズなどのATMスイッチでは無効です。これらのデバイスについては、セクションIを参照してください。

   この回避策により、ILMIコミュニティストリングを使用してデバイスを再設定できるユーザを制限しながら、ATMに対するILMIの機能を継続できます。
   a. 次のコマンドを使用して、アクセスを拒否する簡単なACLを作成します。「66」がすでに使用されている場合は、別の2桁の番号を選択します。
      アクセスリスト66 deny any
   b. 一般にILMIコミュニティに適用して、そのビューを制限します。
      snmpコミュニティILMIビュー*ilmi RW 66
      *ilmiビューが存在しない場合、エラーが報告されます。その場合は、次のコマンドを使用してILMIビューを明示的に制限します。
      snmpコミュニティILMI RW 66
      上記のコマンドで永続的なエラーが発生する場合、この回避策はこのデバイスには適用できません。上記の最初の項目に示されているデフォルトの回避策を使用します。
5. 該当するIOS 11.3(9) ~ 12.0(2)TのリリースでATMを必要としない場合：
   この範囲のすべてのバージョンのIOSはこの回避策を受け入れます。ただし、デバイスをリブートしても変更内容は保持されません。これらの手順は、該当デバイスのシステムをリロードするたびに再適用する必要があります。
   a. ドキュメントに記載されていないILMIコミュニティストリングを公開し、変更できるようにします。
      snmpサーバコミュニティILMI RW
      上記のコマンドを実行すると、エラーが発生する場合がありますが、無視しても問題

はありません。

b. 同じコミュニティの読み取り/書き込み機能を無効にします。
no snmp-server community ILMI RWコマンド
エラーが表示された場合は、この回避策をデバイスに適用できません。この手順を停止し、上記の最初の項目に示されているデフォルトの回避策を使用します。

c. この設定は、システムのリロード後も有効になりません。このコマンドは、システムを再起動するたびに再入力する必要があります。

6. ATMを必要とするIOS 11.3(9)から12.0(2)Tの該当リリースについては、次の手順を実行します。

注：この回避策は、LS1010や8500シリーズなどのATMスイッチでは無効です。この回避策は、12.0(3)T以降に基づく12.0リリース（12.0Sなど）にも有効ではありません。これらのデバイスについては、セクションIを参照してください。

この回避策により、ILMIコミュニティストリングを使用してデバイスを再設定できるユーザを制限しながら、ATMに対するILMIの機能を継続できます。

a. 次のコマンドを使用して、アクセスを拒否する簡単なACLを作成します。「66」がすでに使用されている場合は、別の2桁の番号を選択します。
アクセスリスト66 deny any

b. 一般にILMIコミュニティに適用して、そのビューを制限します。
snmpコミュニティILMIビュー*ilmi RW 66
*ilmiビューが存在しない場合、エラーが報告されます。その場合は、次のコマンドを使用してILMIビューを明示的に制限します。
snmpコミュニティILMI RW 66
上記のコマンドで永続的なエラーが発生する場合、この回避策はこのデバイスには適用できません。上記の最初の項目で説明されているデフォルトの回避策を使用してください。

7. 該当するIOS 12.0(3)T以降のリリースの場合：
これらのIOSリリースには、この回避策に必要なSimple Network Management Protocol(SNMPv3)バージョン3のサポートが含まれています。
snmp-serverコマンドを実行するオプションについてコンソールCLI（コマンドラインインタープリタ）で支援を求め、SNMPv3サポートが存在することを確認します。configモードに入り、次に示すコマンドを入力して、予想される応答を記録します。
snmp-server user test ?

```
remote  Specify a remote SNMP entity to which the user belongs
v1      user using the v1 security model
v2c     user using the v2c security model
v3      user using the v3 security model
```

上記のコマンドで期待どおりの結果が得られなかった場合、SNMPv3はこのリリースではサ

ポートされておらず、この回避策は適用できません。この手順を中止し、上記の最初の項目で説明したデフォルトの回避策を適用することを検討してください。
それ以外の場合、デバイスが期待どおりに応答したら、次の説明と手順に進みます。
これらのIOSリリース(12.0(3)T以降)では、ILMIパケットは通常のIP SNMPパケットと同じ方法でSNMPエンジンによって処理されます。ILMIコミュニティストリングに適用されるアクセスコントロールリストまたはビューは、トランスポートがILMIまたはIPのどちらであっても処理されます。ただし、コミュニティストリングに適用できるアクセスコントロールリストのタイプはIPアクセスリスト文を介するものだけで、この文を適用するとILMIパケットを含むIP以外のすべてのパケットがブロックされます。*ilmiビューを変更または削除すると、ILMIによって転送されるパケットにも影響するため、ビューを変更する回避策は、SNMPを拒否する一方でILMIを許可する場合にも同様に効果がありません。このリリースの範囲では、IP SNMPパケットを拒否し、ILMI SNMPパケットも拒否しない回避策は適用できません。

8. 該当するIOS 12.0(3)T以降のリリースでATMを必要としない場合：
   a. ドキュメントに記載されていないILMIコミュニティストリングを公開し、変更できるようにします。
      snmpサーバコミュニティILMI RW
      上記のコマンドを実行すると、エラーが発生する場合がありますが、無視しても問題はありません。
   b. 同じコミュニティの読み取り/書き込み機能を無効にします。
      no snmp-server community ILMI RWコマンド
      エラーが表示された場合は、この回避策をデバイスに適用できません。この手順を停止し、デフォルトの回避策の使用を検討してください。
9. ATMを必要とするIOS 12.0(3)T以降の該当リリースについては、次の手順を実行します。

   注：このセクションは、LS1010や8500シリーズなどのATMスイッチソフトウェアにも適用されます。このセクションは、12.0(3)T以降に基づくその他の12.0リリース（12.0Sなど）にも適用されます。

   このカテゴリのシステムに有効な回避策は、デフォルトの回避策だけです。
   a. すべてのホストからのSNMPをブロックしている脆弱なデバイスのすべてのインターフェイスにアクセスリストを適用する（デバイスを管理する権限を持つホスト以外）。
   b. 望ましくないSNMPトラフィックが脆弱性のあるデバイスを含むネットワークに入るのを防ぐために、ネットワークのエッジでSNMPアクセスをブロックする。

アクセスリストは、ネットワークの動作とパフォーマンスに与える可能性のある影響を慎重に考慮して導入する必要があります。また、IP送信元アドレスに基づく認証は脆弱であるため、前述の方法では、IP送信元アドレスがスプーフィングされている特定の種類の攻撃から保護できないことに注意してください。
このリリースの範囲では、ILMI SNMPパケットを許可しながらIP SNMPパケットをブロックすることはできません。前述の代替回避策を使用すると、ATM ILMI通信に障害が発生し、設定時にただちにATM接続が失われるか、または後で予期しない接続が失われることが

発生します。デフォルトの回避策を使用するか、修正済みソフトウェアにアップグレードします。

修正済みソフトウェア

次の表に、影響を受けることが分かっているCisco IOSソフトウェアリリースと、修正済みリリースの提供が可能になる最も早い予定日をまとめます。すべての日付は暫定的なものであり、変更される可能性があります。

表の各行に、リリース群、および対象のプラットフォームまたは製品を示します。特定のリリーストレインに脆弱性が存在する場合、修正を含む最初のリリースと予想される日付

リリースを選択するときは、次の定義を念頭においてください。

- Maintenance：テストを重ね、推奨される、表の特定の行にあるラベルのリリース。
- 再構築- 同じリリース群の以前のメンテナンス リリースまたはメジャー リリースから構築されたリリース。特定の障害に対する修正が含まれています。テストの回数は少なくなりますが、修復に必要な最小限の変更のみが含まれています。
- Interim：メンテナンスリリース間の間隔で定期的に構築され、テストの頻度は少なくなります。暫定は、脆弱性に対応しているリリースが他にない場合にだけ選択してください。暫定リリースは、通常、事前の取り決めがない限り、CCO経由でお客様がダウンロードすることはできません。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が不明な場合は、次のセクションに示すように、Cisco TACに連絡して支援を求めてください。

IOSのリリース名と省略形の詳細については、http://www.cisco.com/warp/public/620/1.htmlを参照してください。

リリース群	イメージまたはプラットフォームの説明	修正リリースのアベイラビリティ		
11.xベースのリリース		リビルド	暫定	メンテナンス
10.3 以前	すべて	Not affected		
11.0 ベースのリリース		リビルド	暫定	メンテナンス

11.0	すべてのプラットフォーム用のメジャーGDリリース	11.0(22a) 2001年3月19日		
11.1 ベースのリリース		リビルド	暫定	メンテナンス
11,1	すべてのプラットフォームのメジャーリリース	11.1(24a) 2001年3月19日		
11.1AA	アクセスサーバ用EDリリース：1600、3200、および5200シリーズ。			12.1(7) 2001年2月26日
11.1CA	7500、7200、7000、およびRSPのプラットフォーム固有のサポート	11.1(36)CA1 2001年3月2日		
11.1CC	ISPトレイン：7500、7200、7000、およびRSPでのFIB、CEF、およびNetFlowのサポートを追加	11.1(36)CC1 2001年3月2日		
11,1CT	7500、7200、7000、およびRSPでのタグスイッチングのサポートを追加	12.0(11)ST2 2001年2月26日		

11.1IA	DistributedDirectorのみ	11.1(28)IA1 2001年3月2日		
11.2 ベースのリリース		リビルド	暫定	メンテナンス
11.2	メジャーリリース、一般導入	11.2(25a) 2001年3月5日		
11.2BC	7500、7000、およびRSPでのIBMネットワーキング、CIP、およびTN3270のプラットフォーム固有のサポート			12.1(7) 2001年2月26日
11.2GS	12000 GSRをサポートする早期導入リリース	12.0(15)S1 2001年2月20日		
11.2P	新しいプラットフォームのサポート	11.2(25a)P 2001年3月5日		
11.2SA	Catalyst 2900XLスイッチのみ			12.0(5)WC 2001年4月12日

11.2WA3	LS1010 ATMスイッチ		12.0(10)W(18b)	12.0(13)W5(19b)
			Available	Available
11.2(4)XA	1600および3600の初期リリース	11.2(25a)P		
		2001年3月5日		
11.2(9)XA	5300の初期リリースと3600のデジタルモデムサポート	11.2(25a)P		
		2001年3月5日		
11.3 ベースのリリース		リビルド	暫定	メンテナンス
11.3	すべてのプラットフォームのメジャーリリース	2001年3月5日		
		2001年3月5日		
11.3AA	ダイヤルプラットフォームおよびアクセスサーバ用ED:5800、5200、5300、7200	11.3(11a)AA		
		2001年3月5日		
11.3DA	ISP DSLAM 6200プラットフォームの初期導入トレイン	12.1(5)DA1		
		2001年3月19日		

11.3 DB	6400用のISP/Telco/PTT xDSLブロードバンドコンセントレータプラットフォーム(NRP)の初期配備トレイン	12.1(4)DB1 2001年2月27日		
11.3HA	ISR 3300用の短期EDリリース（SONET/SDHルータ）	脆弱性なし		
11.3 MA	MC3810機能のみ	11.3(1)MA8 2001年3月19日		
11.3NA	Voice over IP、メディアコンバージェンス、各種プラットフォーム	12.1(7) 2001年3月5日		
11.3T	早期導入者向けの豊富な機能を備えた早期導入メジャーリリース	11.3(11b)T1 2001年3月5日		
11.3WA4	LS1010のマルチレイヤスイッチングおよびMultiprotocol over ATM機能		12.0(10)W(18b) Available	12.0(13)W5(19b) Available
	ubr7246および2600の概要	11.3(11b)T1		

		2001年3月5日		
12.0 ベースのリリース		リビルド	暫定	メンテナンス
12.0	すべてのプラットフォーム向けの一般導入リリース		12.0（7.1）	12.0(8)
			Available	Available
12.0DA	xDSLサポート：6100、6200		12.0(7.1)T	
			Available	
12.0DB	ISP/Telco/PTT xDSLブロードバンドコンセントレータプラットフォーム	12.1(4)DB1		
		2001年2月26日		
12.0DC	6400アクセスコンセントレータ	12.1(4)DC2		
		2001年2月26日		
12.0S	コア/ISPサポート：GSR、RSP、c7200	12.0(15)S1		
		2001年2月20日		
12.0SC	ケーブル/ブロードバンドISP:ubr7200			12.0(15)SC
				2001年3月5日

12.0SL	10000 ESR:c10k	12.0(14)SL1		
		2001年2月26日		
12.0ST	すべてのプラットフォーム向けの一般導入リリース	12.0(11)ST2		
		2001年2月26日		
12.0T	Early Deployment(ED):VPN、Distributed Director、各種プラットフォーム			12.1(7)
				2001年2月26日
12.0W5	cat8510c、ls1010、cat8510m			12.0(10)W5(18c)
				Available
	cat8540c、cat8540m			12.0(10)W5(18b)
				Available
	cat5atm、c6msm			12.0(13)W5(19)
				Available
	cat2948g-L3			12.0(10)W5(18e)
				Available

	cat4232			12.0(10)W5(18f)
				Available
	cat4840g			12.0(10)W5(18)
				Available
12.0WT	cat4840g			12.0(13)WT6(1)
				2001年3月15日
12.0XA	Early Deployment(ED)：プラットフォームが限られている			12.1(7)
				2001年2月26日
12.0XB	短期初期配備リリース			12.1(7)
				2001年2月26日
12.0XC	Early Deployment(ED)：プラットフォームが限られている			12.1(7)
				2001年2月26日
12.0XD	Early Deployment(ED)：プラットフォームが限られている			12.1(7)
				2001年2月26日
12.0XE	Early Deployment(ED)：プラ	12.1(5c)E8		

	ットフォームが限られている	2001年3月5日		12.1(7)
12.0XF	Early Deployment(ED)：プラットフォームが限られている			2001年2月26日
12.0XG	Early Deployment(ED)：プラットフォームが限られている			12.1(7) 2001年2月26日
12.0XH	Early Deployment(ED)：プラットフォームが限られている	12.0(4)XH5 2001年3月12日		
12.0XI	Early Deployment(ED)：プラットフォームが限られている			12.1(7) 2001年2月26日
12.0XJ	Early Deployment(ED)：プラットフォームが限られている			12.1(7) 2001年2月26日
12.0XK	Early Deployment(ED)：プラットフォームが限られている	12.0(7)XK4 2001年3月26日		
12.0XL	Early	12.0(4)XH5		

	Deployment(ED)：プラットフォームが限られている	2001年3月12日		12.1(7)
12.0XM	短期初期配備リリース			2001年2月26日
12.0XN	Early Deployment(ED)：プラットフォームが限られている			
12.0XP	Early Deployment(ED)：プラットフォームが限られている	脆弱性なし		
12.0XQ	短期初期配備リリース			12.1(7) 2001年2月26日
12.0XR	短期初期配備リリース	12.1(5)T5 2001年3月5日		
12.0XS	短期初期配備リリース	12.1(5c)E8 2001年3月5日		
12.0XU	Early Deployment(ED)：プラットフォームが限られ	脆弱性なし		

	ている			
12.0XV	短期初期配備リリース	12.1(5)T5 2001年3月5日		
12.0XW	Early Deployment(ED)：プラットフォームが限られている	脆弱性なし		
12.1ベース以降のリリース		リビルド	暫定	メンテナンス
すべての12.1リリース	各種プラットフォーム	脆弱性なし		
注意事項				
*すべての日付は概算であり、変更される可能性があります。 通常のメンテナンス リリースと比較した場合、暫定リリースに対しては厳格なテストが実施されていないため、重大なバグが含まれている可能性があります。				

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

この脆弱性は、シスコのお客様のエンジニアリングスタッフに知られています。シスコは、この通知の公表前に、この情報が一般に知られているものと見なします。

シスコは、この脆弱性の結果として発生したと思われる、ルータの不正な変更に関連する最近のインシデントを認識しています。ただし、これは脆弱性のテストによる意図しない副作用である

可能性があります。

シスコは、この脆弱性を利用するために特別に設計された利用可能なツールを認識していません。ただし、さまざまな市販のネットワーク管理プログラムを使用して、この脆弱性を簡単にテストし、不正利用することができます。クラッカーコミュニティに知られている広く利用可能な特定のプログラムは、この脆弱性の悪用を自動化するために、合理的に有能なプログラマによって変更される可能性があります。

シスコは、上記の例外を除き、この脆弱性に関する一般的な公開討論を行っていません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010227-ios-snmp-ilmi

改訂履歴

Revision 1.5	2001年3月7日	修正済みリリースのバージョンを表で修正
リビジョン 1.4	2001年3月2日	修正済みリリースのバージョンを表で修正
リビジョン 1.3	2001年2月28日	修正済みリリースのバージョンを表で修正、明確にするために回避策を修正
リビジョン 1.2	2001年2月27日	該当製品のエラーを修正
リビジョン 1.1	2001年2月27日	回避策でエラーを修正
リビジョン 1.0	2001年2月27日	最初の暫定パブリックバージョン

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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。