Cisco IOSソフトウェアの複数のSNMPコミュニティストリングの脆弱性

アドバイザリーID : cisco-sa-20010228-ios-snmp-community
初公開日 : 2001-02-28 16:00
バージョン 1.2 : 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

Cisco IOS®ソフトウェアおよびCatOSソフトウェアの複数のリリースには、SNMPコミュニティストリングの予想外の作成と公開に関連する、独立した複数の脆弱性が存在します。これらの脆弱性は、影響を受けるデバイスの不正な表示または変更を許可するために不正利用される可能性があります。

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CSCds32217、CSCds16384、CSCds19674、CSCdr59314、CSCdr61016、およびCSCds49183で文書化されています。

各脆弱性に対する特定の回避策に加えて、SNMPアクセスを防止することで、該当するシステムを保護できます。

この通知はhttps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010228-ios-snmp-community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Noticeで説明されている脆弱性は、Cisco IOSソフトウェアまたはCatOSソフトウェアの特定のリリースを実行しているCiscoルータおよびスイッチ製品に存在します。この脆弱性は、該当するリリースを実行しているシスコ製品にのみ存在します。この他のシスコ製品は該当しません。

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、コマンド「show version」を使用して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「Version」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、シスコ製品で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であることを示しています。

```
Cisco Internetwork Operating System Software IOS (tm)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

シスコ製品が該当するかどうかを判断するには、上記の情報を下記の該当するプラットフォームおよびリリースのリストと比較します。

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。

- 800、1000、1005、1400、1600、1700、2500、2600、3600、MC3810、4000、4500、4700、6200、6400 NRP、6400 NSPシリーズシスコルータ。
- ubr900およびubr920ユニバーサルブロードバンドルータ。
- Catalyst 2900 ATM、2900XL、2948g、3500XL、4232、4840g、5000 RSFCシリーズスイッチ
- 5200、5300、5800シリーズアクセスサーバ。
- Catalyst 6000 MSM、6000ハイブリッドモード、6000ネイティブモード、6000スーパーバイザモジュール、Catalyst ATMブレード
- RSM、7000、7010、7100、7200、ubr7200、7500、10000 ESR、および12000 GSRシリーズCiscoルータ。
- DistributedDirector.
- Catalyst 8510CSR、8510MSR、8540CSR、8540MSRシリーズスイッチ

脆弱性を含んでいないことが確認された製品

Cisco IOSソフトウェアが稼働しておらず、このNoticeで説明されている脆弱性の影響を受けないシスコ製品には次のようなものがありますが、これらに限定されるものではありません。

- Cisco PIX ファイアウォール.
- AironetおよびCisco/Aironetワイヤレス製品。
- CSS11000、Cache Engine、およびLocalDirector製品です。
- 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製品（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

これらの脆弱性は、ネットワークデバイスのリモート管理のためのインターネット標準であるSimple Network Management Protocol(SNMP)に関連する機能の不具合によるものです。SNMPは、「コミュニティストリング」と呼ばれる1つ以上のラベルを使用して、デバイスで表示または変更できる「オブジェクト」（変数）のグループを区切ります。このようなグループのSNMPデータは、Management Information Base（MIB；管理情報ベース）と呼ばれるツリー構造に編成されています。1つのデバイスに複数のMIBを接続して1つの大きな構造にすることができ、さまざまなコミュニティストリングを使用して、大きなデータ構造の異なる（オーバーラップしている可能性がある）部分への読み取り専用アクセスまたは読み取り/書き込みアクセスを提供することができます。読み取り専用変数の例としては、インターフェイスを介して送受信されたオクテットの総数を示すカウンタがあります。読み取り/書き込み変数の例としては、インターフェイスの速度やデバイスのホスト名などがあります。

コミュニティストリングは、SNMP、v1、v2cの以前のバージョンのアクセス制御の弱い形式も提供します。（SNMPv3は、強力な認証を使用して改善されたアクセスコントロールを提供し、サポートされている場合はSNMPv1およびSNMPv2cよりも優先されます）。 コミュニティストリングが定義されている場合、要求された操作がデバイスによって許可されるには、基本的なSNMPクエリーでそのコミュニティストリングを指定する必要があります。コミュニティストリングでは、通常、デバイス全体に対する読み取り専用アクセスまたは読み取り/書き込みアクセスが許可されます。場合によっては、特定のコミュニティストリングは、個々のMIBで説明されている読み取り専用オブジェクトまたは読み取り/書き込みオブジェクトの1つのグループに制限されます。

アクセスを制限する追加の設定オプションがない場合、デバイスの単一コミュニティストリングの知識だけで、すべてのオブジェクト（読み取り専用と読み取り/書き込みの両方）にアクセスし、読み取り/書き込みオブジェクトを変更できます。これらの脆弱性の原因となる不具合は、次のように機能ごとにグループ化されています。

1. この不具合は、SNMPv2の「インフォーム」機能の実装によって発生します。この機能には、ステータス情報を共有するための読み取り専用コミュニティストリングの交換が含まれます。該当するデバイスが、「snmp-server host」コマンドなどのSNMP「トラップ」（ロギングメッセージ）を受信するホストを定義するコマンドを処理する場合、保存された設定にまだ定義されていなければ、trap文で指定されたコミュニティも一般的な使用のために設定

されます。これは、以前にコミュニティが削除され、システムがリロードされる前にコンフィギュレーションがメモリに保存されていた場合でも発生します。

2. 読み取り/書き込み(RW)コミュニティストリングは、デバイスの読み取り専用コミュニティストリングを使用してView-based Access Control MIB(VACM)の「ウォーク」、つまりトラバーサルによってデバイスが調べられるときに公開されます。View-based Access Control（CBAC；ビューベースアクセスコントロール）は、バージョン12.0(3)TのIOSに追加されたSNMPv3の機能です。CSCds32217では、IOSでの不具合について説明します。CSCds16384れは、2900XLおよび3500XLスイッチで稼働するIOSに適用されます。また、CSCds19674では、CatalystスイッチでのCatOSでの不具合についても説明します。12.0(12.0(3)T以降)のほとんどのIOSリリースと、ほとんどの12.1リリースには、2900XLおよび3500XLスイッチの12.0(5.2)XUと12.0(5)XW、およびCatalystスイッチのCatOSリリース5.4(1) ~ 5.5(2)と6.1(1)と同様にこの脆弱性が含まれています。
3. ケーブルモデム管理のための新しいケーブル業界標準の実装により、文書化されていない読み書きコミュニティストリング「cable-docsis」が導入されました。これは、DOCSIS準拠のケーブル対応デバイスのみを対象としたものです。DOCSIS互換ケーブルモデムと限定された範囲のIOSリリースのヘッドエンドユニットを除くすべてのデバイスで、誤ってデフォルトで有効になりました。この不具合は、CSCdr59314で文書化されています。この脆弱性は、12.1(3)および12.1(3)Tに基づく非常に限定されたIOSリリースセットに限定され、12.1(4)および12.1(5)Tリリース以降で修正されています。

特定のリリースの各脆弱性のステータスに関する詳細については、次のソフトウェアセクションを参照してください。

IOSに文書化されていないデフォルトの「ILMI」読み取り/書き込みコミュニティストリングが存在するため、SNMPの脆弱性に関する別のCisco Security Advisoryが最近発表されました。この通知と並行して、このアドバイザリ https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010227-ios-snmp-ilmiも参照してください。

回避策

該当するルータまたはスイッチでenableモードを使用している場合は、次の回避策をすべて設定する必要があります。設定を変更するたびに、必ず「write memory」コマンドを使用して変更を保存してください。

CSCdr61016とCSCds49183によって導入された脆弱性の回避策は、snmp-serverホストを設定する前に、snmp-serverホストのコミュニティストリングを設定することです。このコマンドには、このコミュニティストリングに対する必要なアクセス制限が含まれている必要があります。次の例では、「1.2.3.4」はSNMPトラップを受信するホストのIPアドレスです。

<#root>

```
router#
```

```
config term

   ! create access list
router(config)#

access-list 66 deny any

   ! configure community string with access restrictions
router(config)#

snmp-server community public ro 66

   ! configure snmp-server host
router(config)#

snmp-server host 1.2.3.4 public

router(config)#

exit

router#write memory
router#
```

同じコミュニティストリングを使用して1つ以上の「snmp-server host」コマンドを入力した後で「snmp-server community」コマンドを入力した場合、それ以外には無関係な不具合CSCdr21997ードがあるため、「snmp-server host」コマンドをすべて再入力する必要があります。後者の不具合では、トラップやインフォームがコミュニティストリングを使用してルータから送信されるのを防ぎます。この不具合は、CSCdr61016と同じIOSリリースの一部（すべてではない）に存在します。

「snmp-server host」コマンドの定義後にコミュニティを完全に削除するには、それらのコミュニティに対応する関連する「snmp-server host」コマンドも削除する必要があります。

CSCds32217とCSCds16384で説明されている脆弱性は、「snmp-server view」コマンドを使用してSNMP-VIEW-BASED-ACM-MIBをポーリングする機能をブロックすることで修正できます。その結果、SNMP-VIEW-BASED-ACM-MIBを参照する機能が制限されるビューが作成されます。このビューは、すべての読み取り専用コミュニティストリングに適用する必要があります。例：

<#root>

```
router#

config term

   ! create view
router(config)#

snmp-server view novacm internet included

   ! block vacmSecurityToGroupEntry table
router(config)#

snmp-server view novacm internet.6.3.16 excluded

   ! apply view to read-only security string
```

```
router(config)#
snmp-server community public view novacm RO
router(config)#
exit
router#
write memory
router#
```

該当するルータまたはスイッチに複数の読み取り/書き込み(RW)コミュニティストリングがすでに含まれている場合は、すべての読み取り/書き込み(RW)コミュニティストリングがSNMP-VIEW-BASED-ACM-MIBを読み取れないようにする必要があります。ビューが適用されていない読み取り/書き込みコミュニティストリングの場合は、新しいビューを作成してコミュニティストリングに適用します。読み取り/書き込み(RW)コミュニティストリングにすでにビューが適用されている場合は、SNMP-VIEW-BASED-ACM-MIBにアクセスできないようにビューを変更します。両方の状況を次に示します。

次の例が既存の設定の一部である場合：

<#root>

```
router#
show running-config

...
snmp-server view oldview internet included
snmp-server view oldview ipRouteTable excluded
snmp-server view oldview ipNetToMediaTable excluded
snmp-server view oldview at excluded
snmp-server community tech view oldview RW
snmp-server community private RW
...
```

その後、次の変更によってSNMP-VIEW-BASED-ACM-MIBが除外されます。

<#root>

```
router#
config term

   ! block vacmSecurityToGroupEntry table in existing view
router(config)#
snmp-server view oldview internet.6.3.16 excluded

   ! create new view
```

```
router(config)#
snmp-server view novacm internet included
router(config)#
snmp-server view novacm internet.6.3.16 excluded
   ! apply new view
router(config)#
snmp-server community private view novacm RW
router(config)#
exit
router#
write memory
router#
```

注：この回避策で最大限の保護を実現するには、該当するスイッチまたはルータ上の既存のすべてのビューを同様の方法で変更する必要があります。

CatOSのCSCds19674に記載されている脆弱性は、「set snmp view」コマンドを使用してSNMP-VIEW-BASED-ACM-MIBへのアクセスを防止することで修正できます。例：

<#root>

```
switch#
set snmp view defaultUserView 1.3.6.1.6.3.16.1.2 excluded nonvolatile
```

「cable-docsis」コミュニティストリングが設定から削除されると、システムのリロード後にCSCdr59314によって自動的に再表示されるようになります。次の回避策は、このコミュニティストリングに対するすべての要求を完全に拒否するアクセスリストステートメントを定義することによって、「cable-docsis」コミュニティストリングの使用を禁止します。

<#root>

```
router#
config term
   ! create access list
router(config)#
access-list 66 deny any
```

```
   ! apply access restrictions to cable-docsis community string
router(config)#

snmp-server community cable-docsis ro 66

router(config)#

exit

router#

write memory

router#
```

修正済みソフトウェア

このセキュリティアドバイザリは、関連する複数の製品セキュリティ脆弱性の組み合わせです。影響を受けるトレインとリリースは、すべてのバージョンで同一ではありませんが、影響を受ける不具合が他のバージョンと交差するリリースの重要なグループがあります。特に断りのない限り、「修正済みリリースのアベイラビリティ」に表示される各ラベルは、その特定のトレインのこれらの不具合をすべて解決するリリースを示します。次の例外に注意してください。

- IOSソフトウェアのメジャーリリースバージョン12.0および11.x以前に基づくIOSリリースは、この通知に記載されている脆弱性の影響を受けません。12.0DA、12.0S、12.0Tなど、12.0のその他すべてのリリースが影響を受ける可能性があります。
- CSCdr59314は特定の12.1(3)リリースにのみ存在し、他のIOSリリースには影響しません。
- 6つの不具合すべての修正は、最初のリリースより前に12.2に統合されているため、12.2およびそれ以降のバージョンに基づくすべてのリリースは、このアドバイザリに記載されている不具合の影響を受けません。

次の表に、影響を受けることが確認されているIOSソフトウェアリリースと、推奨される修正済みバージョンの最早提供予定日をまとめます。日付は常に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、各リリースの提供予定日が「Rebuild」、「Interim」、および「Maintenance」の各列に表示されます。特定の列のリリース（最初の修正リリースより前）で特定のトレインのリリースを実行しているデバイスは脆弱であることが確認されており、少なくとも示されたリリース（最初の修正リリースより後）または新しいバージョン（最初の修正リリースより後のラベル）にアップグレードする必要があります。

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。暫定イメージは、脆弱性に対処する適切なリリースが他にない場合にのみ選択し、可能な限り早急に次のメンテナンスリリースにアップグレードする必要があります。暫定リリースは製造部門を通じて入手することはできず、通常はCisco TACと事前に調整を行わないと、CCOからダウンロードできません。

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。

<table>
<tr><th>リリース群</th><th>イメージまたはプラットフォームの説明</th><th colspan="3">修正リリースのアベイラビリティ</th></tr>
<tr><td colspan="2">Catalystソフトウェアリリース</td><td>リビルド</td><td>暫定</td><td>メンテナンス</td></tr>
<tr><td rowspan="2">5.5</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td>5.5(3)</td></tr>
<tr><td>Available</td></tr>
<tr><td rowspan="2">6.1</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td>6.1(2)</td></tr>
<tr><td>Available</td></tr>
<tr><td colspan="2">11.xベースのリリースとそれ以前</td><td>リビルド</td><td>暫定</td><td>メンテナンス</td></tr>
<tr><td>11.x以前</td><td>複数のリリースとプラットフォーム</td><td colspan="3">脆弱性なし</td></tr>
</table>

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General Deploymentリリース	脆弱性なし		
12.0DA	xDSLサポート：6100、6200がCSCds32217に対して脆弱	12.1(5)DA1 2001年3月19日		12.1(6)DA 予定外
12.0DB	すべてのプラットフォーム向けGeneral Deploymentリリース	12.1(4)DB1 2001年2月26日		
12.0DC	すべてのプラットフォーム向けGeneral Deploymentリリース	12.1(4)DC2 2001年2月20日		
12.0S	コア/ISPサポート：GSR、RSP、c7200	12.0(15)S1 2001年2月20日		12.0(16)S 2001年3月19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		12.0(14)SL1		12.0(15)SL
		2001年2月26日		2001年3月19日
12.0ST	すべてのプラットフォーム向けGeneral Deploymentリリース	12.0(11)ST2		12.0(15)
		2001年2月26日		2001年3月5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	Catalystスイッチ：cat8510c、cat8540c、c6msm、ls1010、cat8510m、cat8540m、cat2948g、cat4232	脆弱性なし		
12.0WT	cat4840g	脆弱性なし		
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	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

12.0XC	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)：プラットフォームが限られている	12.1(5c)E8 2001年2月26日		
12.0XF	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
12.0XG	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			12.1(7)

	ットフォームが限られている			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)XK3 2001年3月19日		
12.0XL	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		
12.0XM	短期初期配備リリース			12.1(7) 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			不確定 予定外
12.0XP	Early Deployment(ED)：プラットフォームが限られている	12.0(5)WC 2001年4月13日		

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ている	12.0(5)WC 2001年4月13日		
12.0XW	Early Deployment(ED)：プラットフォームが限られている	12.0(5)WC 2001年4月13日		
12.0XV	短期初期配備リリース	12.1(5)T5 2001年3月5日		12.1WC 2001年4月12日
12.1ベース以降のリリース		リビルド	暫定	メンテナンス

12.1	すべてのプラットフォーム向けの一般導入リリース	12.1(5c)	12.1(5.1)	12.1(7)
		2001年2月20日	Available	2001年2月26日
12.1AA	ダイヤルサポート			12.1(7)AA
				2001年3月12日
12.1DA	xDSLサポート：6100、6200	12.1(5)DA1		12.1(6)DA
		2001年2月28日		2001年2月26日
12.1CX	コア/ISPサポート：GSR、RSP、c7200			12.1(4)CX
				2001年3月13日
12.1DB	すべてのプラットフォーム向けGeneral Deploymentリリース	12.1(4)DB1		12.1(5)DB
		2001年3月5日		2001年3月19日
12.1DC	すべてのプラットフォーム向けGeneral Deploymentリリース	12.1(4)DC2		12.1(5)DC
		2001年3月5日		2001年3月19日
12.1E	コア/ISPサポート：GSR、RSP、c7200	12.1(5c)E8		12.1(6)E

		2001年3月5日		2001年3月12日
12.1EC	コア/ISPサポート：GSR、RSP、c7200	12.1(5)EC1 2001年2月26日		12.1(6)EC 2001年3月26日
12.1EX	コア/ISPサポート：GSR、RSP、c7200	12.1(5c)EX 2001年3月12日		
12.1EY	Cat8510c、Cat8510m、Cat8540c、Cat8540m、LS1010	Not affected		
12.1T	Early Deployment(ED):VPN、Distributed Director、各種プラットフォーム	12.1(5)T5 2001年3月5日		
12.1XA	Early Deployment(ED)：プラットフォームが限られている	12.1(5)T5 2001年3月5日		
12.1XB	Early Deployment(ED)：プラットフォームが限られている	12.1(5)T5 2001年3月5日		

12.1XC	Early Deployment(ED)：プラットフォームが限られている	12.1(5)T5 2001年3月5日		
12.1XD	Early Deployment(ED)：プラットフォームが限られている	12.1(5)T5 2001年3月5日		
12.1XE	Early Deployment(ED)：プラットフォームが限られている	12.1(5)T5 2001年3月5日		
12.1XF	Early Deployment(ED):811および813（c800イメージ）	12.1(2)XF3 2001年3月5日		
12.1XG	早期導入(ED):800、805、820、1600	12.1(3)XG4 2001年3月5日		
12.1XH	Early Deployment(ED)：プラットフォームが限られている	12.1(2)XH5 2001年3月12日		
12.1XI	Early Deployment(ED)：プラ	12.1(3a)XI6		

	ットフォームが限られている	2001年3月19日		不確定
12.1XJ	Early Deployment(ED)：プラットフォームが限られている			予定外
12.1XK	Early Deployment(ED)：プラットフォームが限られている	12.1(5)T5 2001年3月5日		
12.1XL	Early Deployment(ED)：プラットフォームが限られている	12.1(3)XL1 2001年3月5日		
12.1XM	短期初期配備リリース	12.1(5)XM1 2001年2月28日		
12.1XP	Early Deployment(ED):1700およびSOHO	12.1(3)XP3 2001年3月5日		
12.1XQ	短期初期配備リリース	12.1(3)XQ3 2001年3月		

12.1XR	短期初期配備リリース	12.1(5)XR1 2001年2月20日		
12.1XS	短期初期配備リリース			12.1(5)XS 2001年3月12日
12.1XT	Early Deployment(ED):1700シリーズ	12.1(3)XT2 2001年3月5日		
12.1XU	Early Deployment(ED)：プラットフォームが限られている	12.1(5)XU1 2001年2月15日		
12.1XV	短期初期配備リリース	12.1(5)XV1 2001年3月12日		
12.1XW	短期初期配備リリース	12.1(5)XW2 2001年3月6日		
12.1XX	短期初期配備リリース	12.1(5)XX3		

		2001年3月 6日		
12.1XY	短期初期配備リリース	12.1(5)XY4 2001年3月 6日		
12.1XZ	短期初期配備リリース	12.1(5)XZ2 2001年3月 6日		
12.1YA	短期初期配備リリース	12.1(5)YA1 2001年3月 6日		
12.1YB	短期初期配備リリース			12.1(5)YB 2001年2月 13日
12.1YC	短期初期配備リリース			12.1(5)YC 2001年3月 12日
12.1YD	短期初期配備リリース			12.1(5)YD 2001年3月 12日

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

CSCdr59314は内部で発見され、修復されました。シスコでは、「cable-docsis」コミュニティストリングを使用して、お客様のルータが許可なしに変更されたインシデントを認識しています。この脆弱性は、お客様からインシデントが報告された際に、Cisco Product Security Incident Response Team(PSIRT)の注目を集めました。その他の脆弱性は、最初は1つの製品に関してお客様から報告されたか、修復中に他の製品に関して内部的に確認されました。

シスコでは、これらの脆弱性を利用するために設計された特定のプログラムまたはスクリプトについては認識していませんが、このNoticeで説明されている脆弱性を利用するために現状のまま使用したり変更したりできる市販のプログラムやスクリプトは数多く存在します。

シスコでは、公開フォーラムにおけるこれらの脆弱性に関する一般的な議論は確認しておりません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010228-ios-snmp-community

改訂履歴

リビジョン 1.2	2001年3月7日	修正済みバージョン番号を含むソフトウェアテーブルの改訂。誤植を修正。
リビジョン 1.1	2001年3月2日	修正済みバージョン番号を含むソフトウェアテーブルの改訂

リビジョン 1.0	2001年2月28日	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。

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。