Cisco Industrial Ethernet 3000シリーズスイッチにおけるハードコードされたSNMPコミュニティ名の脆弱性

アドバイザリーID : cisco-sa-20100707-snmp
初公開日 : 2010-07-07 16:00
バージョン 1.1 : Final
CVSSスコア : 10.0
回避策 : No Workarounds available
Cisco バグ ID : CSCtf25589

CVE-2010-1574

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®ソフトウェアリリース12.2(52)SEまたは12.2(52)SE1が稼働するCisco Industrial Ethernet 3000(IE 3000)シリーズスイッチには、既知のSNMPコミュニティ名が読み取りアクセスと書き込みアクセスの両方に対してハードコードされている脆弱性があります。ハードコードされたコミュニティ名は「public」と「private」です。

シスコでは、すべての管理者が「回避策」セクションで説明されている緩和策を導入するか、Cisco IOSソフトウェアのアップグレードを実行することを推奨しています。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。

この脆弱性に対しては回避策があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100707-snmp で公開されています。

該当製品

次の製品はこの脆弱性の影響を受けます。

- Cisco Industrial Ethernet 3000 シリーズ スイッチ

脆弱性のある製品

Cisco Industrial Ethernet 3000シリーズスイッチは、次のいずれかのCisco IOSソフトウェアリ

リースを実行している場合に脆弱性が存在します。

- Cisco IOSソフトウェアリリース12.2(52)SEまたは12.2(52)SE1

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。

脆弱性が存在するCisco IOSソフトウェアバージョンを実行しているシスコのスイッチング製品の他のハードウェアモデルは、この脆弱性の影響を受けません。

上記のCisco IOSソフトウェアリリースが稼働していないCisco Industrial Ethernet 3000シリーズスイッチには、脆弱性は存在しません。

詳細

該当するバージョンのCisco IOSソフトウェアを実行しているCisco Industrial Ethernet 3000シリーズスイッチには、ハードコードされたSNMP読み取り/書き込みコミュニティ名が含まれています。

Cisco Industrial Ethernet 3000シリーズは、過酷な環境に適した堅牢で使いやすくセキュアなインフラストラクチャを提供するスイッチファミリです。

SNMPはデバイスの管理と監視に使用され、コミュニティ名はパスワードに相当します。

ハードコードされたSNMPコミュニティ名は次のとおりです。

```
snmp-server community public RO
snmp-server community private RW
```

SNMPコミュニティ名は削除できますが、ハードコードされたコミュニティ名は、デバイスのリロード時に実行コンフィギュレーションに再適用されます。シスコでは、デバイスのリロード時にコミュニティ名が削除されるようにする回避策を提供しています。

注：アクセスリストまたは制限付きMIBビューの設定：

```
snmp-server community public RO 99
snmp-server community private RW 99
snmp-server community public view <mib> RO 99
snmp-server community private view <mib> RO 99

access-list 99 deny   any
```

この手順は、デバイスがリロードされるまでの回避策として機能します。デバイスがリロードされると、コミュニティ名にアクセスリストまたはMIBビューが割り当てられずに、元の設定が挿入されます。このアドバイザリの「回避策」セクションを参照してください。

この脆弱性は、PROFINETと呼ばれる該当リリースに統合された新機能の一部として導入されました。このアドバイザリが公開された時点では、PROFINETはCisco Industrial Ethernet 3000シリーズスイッチでのみサポートされていました。

この脆弱性は、Cisco Bug ID CSCtf25589 (登録ユーザ専用)に記載されています。この脆弱性に対してCommon Vulnerabilities and Exposures(CVE)IDとしてCVE-2010-1574が割り当てられています。

回避策

SNMPコミュニティ名の手動削除

注：次の回避策は、デバイスがリロードされるまで有効です。デバイスをリロードするたびに、この回避策を再適用する必要があります。シスコでは、この脆弱性の恒久的な修正プログラムとしてCisco IOSソフトウェアのアップグレードを実施することを推奨しています。

デバイスにログインし、コンフィギュレーションモードに入ります。次の設定コマンドを入力します。

```
no snmp-server community public RO
no snmp-server community private RW
```

設定を保存すると、スタートアップコンフィギュレーションファイルが更新されますが、ハードコードされたコミュニティ名は、デバイスのリロード時に実行コンフィギュレーションに再挿入されます。この回避策は、デバイスをリロードするたびに適用する必要があります。

SNMPコミュニティ名の自動削除

Embedded Event Manager(EEM)ポリシーを作成すると、デバイスがリロードされるたびに、ハードコードされたSNMPコミュニティ名を自動的に削除できます。次の例は、デバイスがリロードされるたびに実行され、ハードコードされたSNMPコミュニティ名が削除されるEEMポリシーを示しています。

```
event manager applet cisco-sa-20100707-snmp
 event timer countdown time 30
 action 10 cli command "enable"
 action 20 cli command "configure terminal"
 action 30 cli command "no snmp-server community public RO"
 action 40 cli command "no snmp-server community private RW"
```

```
 action 50 cli command "end"
 action 60 cli command "disable"
 action 70 syslog msg "Hard-coded SNMP community names as per Cisco Security Advisory cisco-sa-20100707
```

EEMポリシーの詳細については、http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview_ps6441_TSD_Products_Configuration_Guide_Chapter.htmlにある『Cisco IOS Network Management Configuration Guide - Embedded Event Manager Overview』を参照してください。

インフラストラクチャ アクセス コントロール リスト

ネットワークを通過するトラフィックをブロックすることは往々にして困難ですが、インフラストラクチャデバイスに決して許可すべきではないトラフィックを識別し、そのトラフィックをデバイスインターフェイスまたはネットワークの境界でブロックすることは可能です。

IE3000でSNMP管理が必要ない場合は、すべてのSNMPトラフィックをデバイスにドロップすれば十分です。次のiACLは、レイヤ3アクセスが設定された2つのインターフェイスを持つIE3000の例を示し、IE3000宛てのすべてのSNMPクエリーをドロップします。

```
!---
!--- Deny SNMP traffic from all other sources destined to
!--- configured IP addresses on the IE3000.
!---

access-list 150 deny udp any host 192.168.0.1 eq snmp
access-list 150 deny udp any host 192.168.1.1 eq snmp

!---
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and configurations
!--- Permit all other traffic to transit the device.
!---

access-list 150 permit ip any any

!---
!--- Apply access-list to all Layer 3 interfaces
!--- (only two examples shown)
!---

interface Vlan1
 ip address 192.168.0.1 255.255.255.0
 ip access-group 150 in

interface GigabitEthernet1/1
 ip address 192.168.1.1 255.255.255.0
```

```
ip access-group 150 in
```

ホワイトペーパー『Protecting Your Core: Infrastructure Protection Access Control Lists』には、アクセスリストによるインフラストラクチャ保護のガイドラインと推奨される導入方法が記載されています。このWhite Paperは、http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtmlで入手できます。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリを参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイス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を確認する必要があります。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、Cisco IOS のリリース トレインが記載されています。特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（および、それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。シスコでは、表の「First Fixed Release」列で指定されているリリース、またはそれ以降のリリースにアップグレードすることを推奨しています。

メジャー リリース	修正済みリリースの入手可能性
Affected 12.0-Based Releases	First Fixed Release（修正された最初のリリース）
該当する 12.0 ベースのリリースはありません。	
Affected 12.1-Based Releases	First Fixed Release（修正された最初のリリース）

該当する 12.1 ベースのリリースはありません。	
Affected 12.2-Based Releases	First Fixed Release（修正された最初のリリース）
12.2SE	12.2(52)SEより前のリリースには脆弱性はありません。最初の修正はリリース12.2(55)SEです。現在は2010年8月に利用可能になる予定です。
他に該当する12.2ベースのリリースはありません	
Affected 12.3-Based Releases	First Fixed Release（修正された最初のリリース）
該当する 12.3 ベースのリリースはありません。	
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）
該当する 12.4 ベースのリリースはありません。	
影響を受ける 15.0 ベースのリリース	First Fixed Release（修正された最初のリリース）
影響を受ける 15.0 ベースのリリースはありません。	
影響を受ける 15.1 ベースの	First Fixed Release（修正された最初のリリース）

リリース	
影響を受ける 15.1 ベースのリリースはありません。	

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

この脆弱性は、カスタマーサポートコールの対応時に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100707-snmp

改訂履歴

リビジョン 1.0	2010年7月7日	初回公開リリース

利用規約

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。