Cisco Industrial Ethernet 3000 シリーズ スイッチ脆弱性のハードコードされた SNMPコミュニティ名前

Critical

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 産業イーサネット 3000 （ Cisco IOS® ソフトウェア リリース 12.2(52)SE または 12.2(52)SE1 が稼働している 3000 ） IE シリーズ スイッチはよく知られている な SNMPコミュニティ名前が両方のためにハードコードされている*読み書きアクセス*脆弱性が含まれています。ハードコードされたコミュニティ名はです「パブリック」および「private」。

Cisco 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軽減手段を展開するか、または Cisco IOS ソフトウェア アップグレードを行うことを推奨します。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。

この脆弱性を軽減する回避策は利用できます。

このアドバイザリは 707-snmp で掲示されます。

該当製品

以下の製品はこの脆弱性から影響を受けます:

- 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 スイッチはの次の Cisco IOS ソフトウェア リリース実

行するとき脆弱です:

- Cisco IOS ソフトウェア リリース 12.2(52)SE か 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 な Cisco IOS ソフトウェア バージョンを実行している Cisco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から影響を受けません。

Cisco IOS ソフトウェア リリースを実行していない Cisco Industrial Ethernet 3000 シリーズ スイッチは上でリストされている脆弱ではないです。

詳細

Cisco IOSソフトウェアの影響を受けたバージョンを実行している Cisco Industrial Ethernet 3000 シリーズ スイッチはハードコードされた SNMP 読み書きコミュニティ名前が含まれています。

Cisco 産業イーサネット 3000 シリーズは険しいの、使いやすい提供するスイッチの系列、粗い環境のための安全なインフラストラクチャです。

SNMP は管理のために使用され、監視してデバイスおよびコミュニティ名はパスワードへ等量です。

ハードコードされた SNMPコミュニティ名前は次のとおりです:

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

SNMPコミュニティ名前は取除くことができます; ただし、ハードコードされたコミュニティ名は実行コンフィギュレーションに時デバイスのリロード再適用されます。 Cisco はコミュニティ名を取除かれるときデバイスのリロード確認する回避策を提供しました。

注: アクセス リストか制限 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
```

デバイスまでの回避策として進行作業はリロードされます。 デバイスがリロードされればオリジナル設定はコミュニティ名に割り当てられるアクセス リストか MIB ビューなしで挿入されます。 このアドバイザリの回避策 セクションを参照して下さい。

この脆弱性は PROFINET と呼ばれた該当するリリースに統合新しい 機能の一部としてもたらされました。 このアドバイザリの出版物の時に、PROFINET はサポートされた on Cisco 産業イーサネット 3000 シリーズ スイッチだけでした。

この脆弱性は Cisco バグ ID **CSCtf25589** （登録ユーザのみ）で文書化されています。 この脆弱性よくある脆弱性および公開（CVE）ID CVE-2010-1574 は割り当てられました。

回避策

手動で SNMPコミュニティ名前を取除いて下さい

注: 次の回避策はデバイスがリロードされるまでだけ有効です。 デバイスの各リロードにこの回避策は再適用する必要があります。 Cisco はこの脆弱性のためのパーマネント修正として Cisco IOS ソフトウェア アップグレードの実行を励まします。

デバイスへのログインは、コンフィギュレーションモードを開始し。 次の設定コマンドを入力して下さい:

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

設定を保存することは始動コンフィギュレーション ファイルをアップデートします; ただしハードコードされたコミュニティ名は実行コンフィギュレーションに時デバイスのリロード再挿入されます。 この回避策はデバイスがリロードされるたびに適用する必要があります。

自動的に SNMPコミュニティ名前を取除いて下さい

組み込みイベント マネージャ（EEM）ポリシーの作成によって、デバイスがリロードされるたびに自動的にハードコードされた SNMPコミュニティ名前を取除くことは可能性のあるです。 次の例は EEM ポリシーがいつも動作するデバイス リロードされ、ハードコードされた SNMPコミュニティ名前を取除く示します。

```
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-snmp removed"
```

EEM に関する詳細についてはポリシーによっては次のリンクで Cisco IOSネットワーク 管理設定ガイドが-組み込みイベント マネージャ概要参照します:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview_ps6441_TSD_Products_Configuration_Guide_Chapter.html。

ネットワークを通過する頻繁にトラフィックをブロックすることは困難であるが、決してインフラストラクチャ デバイスを目標とし、ネットワークのデバイス インターフェイスかボーダーでそのトラフィックをブロックするようにするべきではないトラフィックが識別することは可能性のあるです。

SNMP 管理が IE3000 で必要とならない場合、デバイスへすべての SNMP トラフィックを廃棄することは十分な回避策です。 iACL は下記の IE3000 に向かうすべての SNMP クエリを廃棄するレイヤ3 アクセスで 2 つのインターフェイスが設定されている IE3000 の例を示します:

```
!--- !--- 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
```

コアを保護する白書「: Infrastructure Protection Access Control Lists (ACL) には、インフラストラクチャ保護アクセス リストに関するガイドラインと推奨配備方法が記載されています。 このホワイトペーパーは、以下のリンクから入手可能です。
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml
。

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、顧客は現在のハードウェア および ソフトウェア構成が新しいリリースによってきちんとサポートされ続けること含まれています十分なメモリがアップグレードされるべきデバイスを確認するために注意し。 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。 Cisco は表の「最初修正済みリリース」カラムで規定 される リリースよりまたはそれ以降と等しいリリースにアップグレードすることを推奨します。

メジャー リリ	修正済みリリースの入手可能性

ース	
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 以前のリリースは脆弱ではないです。 リリース 12.2(55)SE で固定される第 1。現在利用可能 な August 2010 であるためにスケジュールされる。
他が該当しました 12.2 基づいたリリースにありません	
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。	
該当する 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)**
該当する 15.0 基づいたリリースがありません	
該当する 15.1 ベースのリリース	**First Fixed Release (修正された最初のリリース)**
該当する 15.1 基づいたリリースがありません	

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の公示か不正利用に気づいていません。

この脆弱性はカスタマー サポートを処理するとき呼出します検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100707-snmp

改訂履歴

リビジョン 1.0	2010-July-07	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。