アクセスポイントのWebブラウザインターフェイスの脆弱性

アドバイザリーID : cisco-sa-20060628-ap CVE-2006-3291
初公開日 : 2006-06-28 17:00
バージョン 1.2 : Final
回避策 : No Workarounds available
Cisco バグ ID : CSCsd67403 CSCsf18032

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アクセスポイントおよびCisco 3200シリーズワイヤレスモバイルインターフェイスカード(WMIC)用のCisco Webブラウザインターフェイスには、特定の状況で管理アクセスポイントからデフォルトのセキュリティ設定を削除し、管理者ユーザのクレデンシャルを検証せずに管理アクセスを許可する可能性のある脆弱性が存在します。

シスコでは、該当するお客様用に、この脆弱性に対応する無償ソフトウェアを提供しております。この脆弱性の影響を軽減する回避策があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060628-ap で公開されています。

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

Cisco IOS®ソフトウェアリリース12.3(8)JA、12.3(8)JA1、または12.3(8)JKを実行していて、Webインターフェイス管理用に設定されている次のアクセスポイントが影響を受けます。

- 350ワイヤレスアクセスポイントおよびワイヤレスブリッジ
- 1100ワイヤレスアクセスポイント
- 1130ワイヤレスアクセスポイント
- 1200ワイヤレスアクセスポイント
- 1240ワイヤレスアクセスポイント
- 1310ワイヤレスブリッジ

- 1410ワイヤレスアクセスポイント
- Cisco 3200シリーズワイヤレスモバイルインターフェイスカード(WMIC)

CiscoアクセスポイントでWebインターフェイス管理が有効になっているかどうかを確認するには、デバイスにログインしてshow ip http server statusコマンドを発行します。出力にhttp server statusまたはhttp secure server statusのいずれかがenabledと表示されている場合、Webインターフェイス管理は有効です。Webインターフェイス管理が有効になっている場合の例を次に示します。

<#root>

ap#

show ip http server status

```
     HTTP server status: Enabled
     HTTP server port: 80
[...lines removed...]
     HTTP secure server status: Disabled
     HTTP secure server port: 443
[...lines removed...]
```

Webインターフェイス管理（HTTPサーバ）はデフォルトで有効になっています。

アクセスポイントで稼働しているCisco IOSのバージョンを確認するには、次の手順を実行します。

- ブラウザ経由:System Softwareメニューをクリックします。Cisco IOSソフトウェアのバージョンがSystem Software Versionフィールドに表示されます。
- コマンドラインインターフェイス(CLI):Ciscoアクセスポイントで稼働しているソフトウェアを判別するには、デバイスにログインし、show versionコマンドを発行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」と表示されます。

出力の次の行には、カッコに囲まれたイメージ名が表示され、その後にバージョンと Cisco IOS リリース名が続きます。その他の Cisco 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、シスコアクセスポイントでCisco IOSソフトウェアリリース12.3(7)JA1が稼働し、インストールされているイメージ名がC1200-K9W7-Mであることを示しています。

<#root>

ap#

```
show version

Cisco IOS Software, C1200 Software (C1200-K9W7-M),
Version 12.3(7)JA1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 06-Oct-05 09:40 by evmiller
!
[...lines removed...]
!
```

Cisco IOSリリースの命名の詳細については、http://www.cisco.com/warp/public/620/1.htmlを参照してください。

脆弱性を含んでいないことが確認された製品

脆弱性を含んでいない製品は次のとおりです。

- Cisco IOSソフトウェアを実行していないアクセスポイント
- Cisco IOSソフトウェアリリース12.3(8)JA、12.3(8)JA1、または12.3(8)JK以外のCisco IOSの任意のバージョンを実行しているアクセスポイント
- Webインターフェイス管理が無効になっているアクセスポイント（HTTPとHTTPの両方でセキュア）
- Lightweightモードで動作するすべてのCiscoアクセスポイント

詳細

Webブラウザインターフェイスには、ワイヤレスデバイスの設定の変更、ファームウェアのアップグレード、ネットワーク上の他のワイヤレスデバイスの監視と設定に使用する管理ページが含まれています。Webブラウザインターフェイスはデフォルトで有効になっており、設定コマンドip http serverまたはip http secure-serverで示されます。

デフォルト設定を実行しているアクセスポイントは、管理アクセスにデフォルトのイネーブルシークレットパスワードを使用します。これは、Webブラウザインターフェイスのタブ**Security > Admin Access > Default Authentication (Global Password)**を使用するか、CLIの設定コマンド enable secret [new_secret] を使用して変更できます。

Local User List Only (Individual Passwords)を使用すると、アクセスポイントの管理者は、共通のグローバルパスワードが共有されないように、ローカルで一意のユーザ名/パスワードデータベースを管理者に定義できます。

Security > Admin Accessの順に選択してDefault Authentication (Global Password)をLocal User List Only (Individual Passwords)に変更すると、アクセスポイントのWebブラウザインターフェイスに脆弱性が存在します。その結果、アクセスポイントはセキュリティなしで再設定され、グローバルパスワードまたは個別パスワードが有効になります。これにより、ユーザクレデンシャルの検証なしで、Webブラウザインターフェイスまたはコンソールポートを介したアクセスポイン

トへのオープンアクセスが可能になります。

ローカルユーザリストのみ（個々のパスワード）に設定され、脆弱性のないバージョンのCisco IOSが稼働していて、引き続き脆弱性のあるバージョンのIOSにアップグレードされるアクセスポイントは、アップグレード後に設定が変更されない限り、この脆弱性の影響を受けません。

この脆弱性は、Cisco Bug ID CSCsd67403(登録ユーザ専用)「Cannot Select Option to Authenticate using Local User List Only」に記載されています。

回避策

この脆弱性の影響を緩和するには、次のいずれかの回避策と緩和策を使用できます。

- Webベースの管理を無効にする
  次の方法でWebブラウザインターフェイスを使用しないようにするには、次の手順を実行します。
  - Web-Based Management:Services > HTTP-Web ServerページでDisable Web-Based Managementチェックボックスを選択し、Applyをクリックします。
  - CLI：デバイスにログインし、次の設定コマンドを発行します（終了時に設定を保存します）。

  ```
  <#root>

  ap(config)#

  no ip http server

  ap(config)#

  no ip http secure-server

  ap(config)#

  exit
  ```

- CLIによる設定
  WebブラウザインターフェイスではなくCLIを介してローカルユーザリストのみ（個々のパスワード）を有効にすると、アクセスポイントに必要な保護設定が提供されます。デバイスにログインし、次の設定コマンドを発行します（終了時に設定を保存します）。

  ```
  <#root>

  ap#

  configure terminal

  !--- Setup the username password pair first.

  ap(config)#
  ```

```
username test privilege 15 password test

!--- Enable AAA.

ap(config)#
aaa new-model

!--- Enable aaa authentication to the local database.

ap(config)#
aaa authentication login default local

!--- Enable aaa authorization to the local database.

ap(config)#
aaa authorization exec default local

!--- Enable http authentication to AAA.

ap(config)#
ip http authentication aaa
ap(config)#
exit
```

- 最初にRADIUS/TACACSサーバを設定する
  この脆弱性は、WebブラウザインターフェイスでSecurity > Server Manager > Corporate Serversの順に選択し、Security > Admin Accessのオプションを Local User List Only (Individual Passwords)として実行することで回避できます。

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も参照して、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、リリース トレインとそれに対応するプラットフォームまたは製品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存在する場合、修正を含む最初のリリース（最初の修正リリース）とそれぞれの提供予定日が「リビルド」列と「メンテナンス」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。このようなリリースは、少なくとも、示されているリリース以上（最初の修正リリース ラベル以上）にアップグレードしてする必要があります。

「リビルド」および「メンテナンス」という用語の詳細については、次のURLを参照してください。http://www.cisco.com/warp/public/620/1.html

メジャー リリース	修正済みリリースの入手可能性	
12.3	リビルド	メンテナンス
12.3(8)JA	12.3(8)JA2	12.3(11)JA
12.3(8)JA1	12.3(8)JA2	12.3(11)JA
12.3(8)JK	脆弱性あり – TACにお問い合わせください。	

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。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060628-ap

改訂履歴

リビジョン	2006年9月20日	「脆弱性が存在する製品」セクションを更新してCisco 3200シリーズワイヤレスモバイルインターフェイスカード

1.2		(WMIC)を追加し、「ソフトウェアバージョンおよび修正」セクションを更新して12.3(8)JKを追加。
リビジョン1.1	2006年7月6日	Cisco IOSソフトウェアリリース12.3(11)JAのリリース日は、「ソフトウェアバージョンと修正」セクションで変更されています。
リビジョン1.0	2006 年 6 月 28 日	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。

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。