Wireless Location Applianceのデフォルトパスワード

severity

アドバイザリーID : cisco-sa-20061012-wla

初公開日 : 2006-10-12 16:00

バージョン 1.0 : 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 Wireless Location Applianceソフトウェアには、「root」管理アカウントのデフォルトパスワードが含まれています。このユーザ名を使用してログインするユーザは、デバイスを完全に制御できます。

このパスワードは、2.1.34.0より前のバージョンで新しい製品購入の一部として出荷されるすべてのインストールで同じです。この脆弱性は、製品の初期インストール後にパスワードを変更する明示的な手順が実行されていない限り、アップグレードされたインストールでも存在します。

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-20061012-wlaで入手できます。

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、2.1.34.0より前のバージョンで出荷されたCisco 2700シリーズワイヤレスロケーションアプライアンスに影響を与えます。

Wireless Location Applianceのソフトウェアのバージョンは、次の3つの方法のいずれかで確認

できます。

コマンドラインからgetserverinfoコマンドを使用してバージョンを確認できます。バージョンは、バージョン1.1.73.0を実行しているデバイスからの次の出力に似た出力の最初の5行に含まれています。

```
-------------
Server Config
-------------
Product name: Cisco Wireless Location Appliance
Version: 1.1.73.0
```

コマンドラインからバージョンを取得するもう1つの方法は、ファイル/opt/locserver/conf/version.txtを表示することです。バージョン2.0.42.0を実行するWLAの場合、そのファイルの内容は次のようになります。

```
[root@locserv /]# cat /opt/locserver/conf/version.txt
#Tue Jan 31 11:08:35 PST 2006
build.number=42
minor.number=0
patch.number=0
major.number=2
branch.name=HOT
product.name=Cisco Wireless Location Appliance
```

バージョンは、「major.number」で始まり、「minor.number」、「build.number」、「patch.number」の順に数字を組み合わせて、数字をピリオドで区切って簡単に得ることができます。

最後に、バージョンは、Cisco Wireless Control System(WCS)に設定されているLocation AppliancenのWebインターフェイスを介して取得できます。「Locations」タブを参照し、表示されるメニューで「Location Servers」をクリックすると、「Versions」列にLocation Applianceとその対応するバージョンのリストが表示されます。

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。

詳細

Cisco Wireless Location Appliance(WLA)は、RFフィンガープリントテクノロジーを使用して、WLANインフラストラクチャ内から直接802.11ワイヤレスデバイスを同時に追跡します。設計上、Cisco Wireless Location Applianceは、CiscoワイヤレスLANコントローラとCisco Aironet Lightweightアクセスポイントを使用してWLANインフラストラクチャに直接統合され、ワイヤレスデバイスの物理的な場所を追跡します。

Cisco Wireless Location Applianceは、仮想端末（アプライアンスに直接接続された標準のキーボードとモニタ）、ローカルシリアルコンソール、リモートSSH接続、および/またはリモートのセキュアWebセッションを介して管理できます。特定の管理、トラブルシューティングタスク、および基本的な初期設定を実行できるように、特別な管理アカウントが用意されています。

管理者ログインのデフォルトのユーザ名は「root」（引用符なし）で、デフォルトのパスワードは「password」（引用符なし）です。ユーザ名とパスワードは、どちらも大文字と小文字が区別されます。

この問題は、修正済みバージョンのソフトウェアでは、アプライアンスのセットアップのインストール中にrootアカウントのパスワードを変更するようユーザに求めることで対処されています。これは、最初のインストール用に脆弱性のないバージョンのソフトウェアが最初に搭載されて出荷された新しいWLAデバイスにのみ適用されます。アップグレードされた以前のバージョンのソフトウェアでは、アップグレード中にrootユーザのパスワードの変更を求めるプロンプトは表示されません。

この問題は、Cisco Bug ID CSCsb92893(登録ユーザ専用)に記述されています。

回避策

このドキュメントで説明されている脆弱性は、影響を受けるWLAにログインし、管理ルートアカウントのデフォルトパスワードをユーザが選択した強力なパスワードに変更することで排除できます。

パスワードを以前に変更していない場合、管理者ログインのデフォルトのユーザー名は「root」（引用符なし）で、デフォルトのパスワードは「password」（引用符なし）です。ユーザ名とパスワードは、どちらも大文字と小文字が区別されます。rootとしてWLAに正常にログインした後、**passwd**コマンドを実行すると、デフォルトのパスワードを変更できます。

新しいパスワードを有効にするためにリブートする必要はないので、ネットワークの動作が中断されることはありません。

修正済みソフトウェア

この脆弱性は、Cisco Wireless Location Applianceソフトウェアの初期インストール用の新しいデバイスに搭載されて出荷された場合に、バージョン2.1.34.0以降で修正されています。

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。

不正利用事例と公式発表

Cisco PSIRTは、Cisco Wireless Location Applianceがデフォルトのルートパスワードによって侵害された事例をいくつか認識しています。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20061012-wla

改訂履歴

リビジョン 1.0	2006年10月12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。