Cisco Wireless LAN Controllerの複数の脆弱性

アドバイザリーID : cisco-sa-20140305-wlc
初公開日 : 2014-03-05 16:00
バージョン 1.0 : Final
CVSSスコア : 10.0
回避策 : No Workarounds available
Cisco バグ ID : CSCuf66202 CSCue87929 CSCuh33240 CSCuh74233 CSCuf80681 CSCuf52361

CVE-2014-0701
CVE-2014-0703
CVE-2014-0705
CVE-2014-0704
CVE-2014-0707
CVE-2014-0706

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 LAN Controller(WLC)製品ファミリは、次の脆弱性の影響を受けます。

- CiscoワイヤレスLANコントローラのDoS脆弱性
- Cisco Wireless LAN Controllerの関連アクセスポイントへの不正アクセスの脆弱性
- Cisco Wireless LAN Controller IGMPバージョン3のDoS脆弱性
- CiscoワイヤレスLANコントローラのMLDv2におけるDoS脆弱性
- CiscoワイヤレスLANコントローラにおける巧妙に細工されたフレームによるDoS脆弱性
- CiscoワイヤレスLANコントローラにおける巧妙に細工されたフレームによるDoS脆弱性

シスコはこれら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。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140305-wlc

該当製品

Cisco WLC製品ファミリは、複数の脆弱性の影響を受けます。影響を受けるCisco WLCソフトウェアのバージョンは、脆弱性によって異なります。

脆弱性のある製品

具体的なバージョン情報については、このアドバイザリの「ソフトウェアバージョンおよび修正」セクションを参照してください。
このセキュリティアドバイザリに記載されている脆弱性のうち少なくとも1つは、次の各製品に影響を与えます。

スタンドアロンコントローラ

- Cisco 500シリーズワイヤレスExpressモビリティコントローラ
- Cisco 2000 シリーズ ワイアレス LAN コントローラ
- Cisco 2100 シリーズ ワイアレス LAN コントローラ
- Cisco 2500 シリーズ ワイヤレス コントローラ
- Cisco 4100 シリーズ ワイアレス LAN コントローラ
- Cisco 4400 シリーズ ワイアレス LAN コントローラ
- Cisco 5500 シリーズ ワイヤレス コントローラ
- Cisco Flex 7500 シリーズ Wireless Controller
- Cisco 8500 シリーズ ワイヤレス コントローラ
- Cisco 仮想ワイヤレス コントローラ

モジュラコントローラ

- Cisco Catalyst 6500シリーズ/7600シリーズWireless Services Module(Cisco WiSM)
- Cisco Wireless Services Moduleバージョン2(WiSM2)
- サービス統合型ルータ(ISR)用Cisco NME-AIR-WLCモジュール
- サービス統合型ルータ(ISR)用Cisco NM-AIR-WLCモジュール
- Cisco Catalyst 3750Gシリーズ統合型WLC
- Services-Ready Engine(SRE)向けCisco Wireless Controllerソフトウェア*

* Integrated Services Module 300およびCisco Services-Ready Engine 700、710、900、910製品を対象としています。

注:Cisco 2000シリーズWLC、Cisco 4100シリーズWLC、Cisco NM-AIR-WLC、およびCisco 500シリーズワイヤレスExpressモビリティコントローラは、ソフトウェアメンテナンスが終了しています。次の表に、各モデルのサポート終了ドキュメントのURLを示します。

モデル	サポート終了ドキュメントのURL

Cisco 2000 シリーズ WLC	http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6308/prod_end-of-life_notice0900aecd805d22b0.html
ISR向け Cisco NM-AIR-WLCモジュール	http://www.cisco.com/en/US/prod/collateral/modules/ps2797/prod_end-of-life_notice0900aecd806aeb34.html
Cisco 500シリーズワイヤレス Expressモビリティコントローラ	http://www.cisco.com/en/US/prod/collateral/wireless/ps7306/ps7320/ps7339/end_of_life_c5568040.html

特定の環境で実行されているCisco WLCソフトウェアのバージョンを確認するには、次のいずれかの方法を使用します。

Webインターフェイスで Monitorタブを選択し、左側のペインで Summaryをクリックして、Software Versionフィールドを確認します。

コマンドラインインターフェイスで、次の例に示すように show sysinfoコマンドを発行します。

<#root>

```
(Cisco Controller)>
show sysinfo


Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 7.4.121.0
Bootloader Version............................... 1.0.16
Field Recovery Image Version..................... 7.0.112.21
Firmware Version................................. FPGA 1.7, Env 1.8, USB console 2.2
```

CiscoワイヤレスLANコントローラのDoS脆弱性

WebAuth機能が有効になっているかどうかを確認するには、設定された各ワイヤレスネットワークに対して show wlan <X>コマンド(X=wlan ID)を実行します。 次の例は、この機能が有効になっていることを示しています。

```
Web Based Authentication..................... Enabled
```

Cisco Wireless LAN Controller IGMPバージョン3のDoS脆弱性

IGMPv3機能が有効になっているかどうかを確認するには、 show network summaryコマンドを発行します。次の例では、この機能が有効になっています。

```
IGMP snooping.............................. Enabled
```

CiscoワイヤレスLANコントローラのMLDv2におけるDoS脆弱性

MLDv2機能が有効になっているかどうかを確認するには、 show network summaryコマンドを発行します。次の例は、この機能が有効になっていることを示しています。

```
MLD snooping.............................. Enabled
```

要約テーブル:

	4.(x)	5.x	6.x	7.0	7.1	7.2	7.3	7.4	7.5	7.6
CiscoワイヤレスLANコントローラのDoS脆弱性 CVE-2014-0701				X		X	X	X		
Cisco Wireless LAN Controllerの関連アクセスポイントへの不正アクセスの脆弱性 CVE-2014-0703								X		
Cisco Wireless LAN Controller IGMPバージョン3のDoS脆弱性 CVE-2014-0704	X	X	X	X	X	X	X	X		

CiscoワイヤレスLANコントローラのMLDv2におけるDoS脆弱性 CVE-2014-0705						X	X	X	X	
CiscoワイヤレスLANコントローラにおける巧妙に細工されたフレームによるDoS脆弱性 CVE-2014-0706						X	X	X		
CiscoワイヤレスLANコントローラにおける巧妙に細工されたフレームによるDoS脆弱性 CVE-2014-0707						X	X	X		
推奨リリース	移行	移行	移行	7.0.250.0	移行	移行	移行	7.4.121.0	移行	7.6.100.0

脆弱性を含んでいないことが確認された製品

次のIOS-XEベースのワイヤレスコントローラは影響を受けません。

Cisco 5700 シリーズ ワイヤレス コントローラ
Cisco 3600 シリーズ ワイヤレス コントローラ
Cisco 3800 シリーズ ワイヤレス コントローラ

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 WLCとCisco WiSMは、セキュリティポリシー、侵入防御、RF管理、Quality of Service(QoS)、モビリティなど、システム全体のワイヤレスLAN機能を担っています。これらのデバイスは、Lightweight Access Point Protocol(LWAPP)およびControl and Provisioning of Wireless Access Points(CAPWAP)プロトコルを使用して、レイヤ2（イーサネット）またはレイヤ3(IP)インフラストラクチャ上のコントローラベースのアクセスポイントと通信します。

Cisco WLCファミリのデバイスは、次の脆弱性の影響を受けます。

CiscoワイヤレスLANコントローラのDoS脆弱性

Cisco Wireless LAN Controller(WLC)のWebAuth機能の脆弱性により、認証されていないリモートの攻撃者がデバイスのリロードを引き起こす可能性があります。

この脆弱性は、WebAuthログインの処理中に使用されたメモリの割り当て解除が失敗することに

起因します。攻撃者は、大量のWebAuth要求を大量に作成し、未完了の状態にしておくことで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はデバイス上の使用可能なメモリをすべて消費する可能性があります。これにより、ウォッチドッグプロセスがWLCを再起動し、その結果、デバイスのリブート中にサービス拒否(DoS)が発生します。

デバイスがこの脆弱性の影響を受けるには、WebAuth機能が有効になっていて設定されている必要があります。この機能はデフォルトで無効になっています。

この脆弱性は、Cisco Bug ID CSCuf52361(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2014-0701が割り当てられています。

Cisco Wireless LAN Controllerの関連アクセスポイントへの不正アクセスの脆弱性

Cisco Wireless LAN Controller(WLC)によってCisco Aironet 1260、2600、3500、および3600シリーズアクセスポイント(AP)にプッシュされるCisco IOSコードの脆弱性により、認証されていないリモートの攻撃者が該当デバイスへの不正な特権アクセスを取得する可能性があります。

この脆弱性は、影響を受けるアクセスポイントの管理HTTPサーバが管理者によって明示的に無効にされていても有効になる可能性のある競合状態に起因します。攻撃者は、ローカルに保存されたAPのクレデンシャルを使用して該当デバイスへの認証を試みることにより、この脆弱性を不正利用する可能性があります。攻撃に成功すると、攻撃者は該当するAPを完全に制御し、設定に対して任意の変更を加えることができます。

多くの導入シナリオでは、ローカルに保存されたデフォルトのAPユーザ名とパスワードが工場出荷時のデフォルトから変更されていません。このようなゼロタッチのシナリオでは、デバイスは自動的にWLCに接続し、ファームウェアと設定をダウンロードするように設計されています。

この脆弱性は、Cisco Bug ID CSCuf66202(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2014-0703が割り当てられています。

Cisco Wireless LAN Controller IGMPバージョン3のDoS脆弱性

Cisco Wireless LAN Controller(WLC)のIGMP処理サブシステムの脆弱性により、認証されていないリモートの攻撃者がDoS状態を引き起こす可能性があります。

この脆弱性は、特定のIGMPメッセージタイプの特定のフィールドの検証が不適切なことに起因します。メッセージが処理されると、IGMPサブシステムはメモリオーバーリードを実行する可能性があります。 関係のないデータに対して後続の処理が実行されると、エラーが発生してデバイスがリロードされる可能性があります。攻撃者は、該当のWLCによって受信および処理されるネットワークに悪意のあるIGMPバージョン3メッセージを注入することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はWLC上で重大なエラーをトリガーし、デバイスの再起動中にDoS状態を引き起こす可能性があります。

IGMPv3スヌーピング機能はデフォルトで無効になっており、管理者が明示的に設定しなければデバイスに脆弱性が存在しません。

この脆弱性は、Cisco Bug ID CSCuh33240(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2014-0704が割り当てられています。

CiscoワイヤレスLANコントローラのMLDv2におけるDoS脆弱性

IPv6用に設定されたCisco WLCのマルチキャストリスナー検出(MLD)サービスの脆弱性により、認証されていないリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、不正なMLDバージョン2メッセージを適切に解析できないことに起因します。攻撃者は、Cisco WLCがリッスンしているマルチキャスト対応ネットワークに不正なMLDv2パケットを送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はWLC上で重大なエラーをトリガーし、デバイスの再起動中にDoS状態を引き起こす可能性があります。

MLDv2スヌーピング機能はデフォルトで無効になっており、管理者が明示的に設定しなければデバイスに脆弱性が存在しません。

この脆弱性は、Cisco Bug ID CSCuh74233(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2014-0705が割り当てられています。

CiscoワイヤレスLANコントローラにおける巧妙に細工されたフレームによるDoS脆弱性

Cisco WLCの脆弱性により、認証されていないリモートの攻撃者が重大なエラーを引き起こし、デバイスの再起動中にDoS状態が発生する可能性があります。

この脆弱性は、イーサネット802.11フレームを正しく処理できないことに起因します。攻撃者は、特別に巧妙に細工されたイーサネット802.11フレームを送信することで、この脆弱性を不正利用する可能性があります。この脆弱性が繰り返し悪用されると、DoS状態が続く可能性があります。

この脆弱性は、Cisco Bug ID CSCue87929(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2014-0706が割り当てられています。

CiscoワイヤレスLANコントローラにおける巧妙に細工されたフレームによるDoS脆弱性

Cisco WLCの脆弱性により、認証されていないリモートの攻撃者が重大なエラーを引き起こし、デバイスの再起動中にDoS状態が発生する可能性があります。

この脆弱性は、イーサネット802.11フレームを正しく処理できないことに起因します。攻撃者は、特別に巧妙に細工されたイーサネット802.11フレームを送信することで、この脆弱性を不正利用する可能性があります。この脆弱性が繰り返し悪用されると、DoS状態が続く可能性があります。

この脆弱性は、Cisco Bug ID CSCuf80681(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2014-0707が割り当てられています

回避策

Cisco Wireless LAN Controllerの関連アクセスポイントへの不正アクセスの脆弱性

管理者は、影響を受けるデバイスでグローバルAP管理クレデンシャルを設定することで、この問題を軽減できます。これにより、デフォルトが無効になり、権限のないユーザがHTTPインターフェイス経由でAPにアクセスできなくなります。

このドキュメントで説明されている他の脆弱性に対するデバイス上での回避策はありません

このアドバイザリに記載されている脆弱性の緩和策に関する情報は、このアドバイザリに関連するApplied Mitigation Bulletin(AMB)のIdentifying and Mitigating Exploitation of Multiple Vulnerabilities in Cisco Wireless LAN Controllers

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の可能性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規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

Ciscoワイヤレスlanコントローラのdos脆弱性		
影響を受けるリリース	最初の修正	推奨
7.0	7.0.250.0	7.0.250.0または7.4.121.0*
7.2	N/A	7.4.121.0 または 7.6.100.0 への移行が必要
7.3	N/A	7.4.121.0 または 7.6.100.0 への移行が必要
7.4	7.4.110.0	7.4.121.0

* 4400/WiSM1/3750/2000コントローラは7.0コードを超えてアップグレードできない

Cisco Wireless LAN Controllerの関連アクセスポイントへの不正アクセスの脆弱性

影響を受けるリリース	最初の修正	推奨
7.4	7.4.110.0	7.4.121.0

Cisco Wireless LAN Controller IGMPバージョン3のDoS脆弱性		
影響を受けるリリース	最初の修正	推奨
4.(x)	N/A	7.0.250.0 に移行
5.x	N/A	7.0.250.0 に移行
6.x	N/A	7.0.250.0 に移行
7.0	7.0.250.0	7.0.250.0または7.4.121.0*への移行が必要
7.1	N/A	7.4.121.0 または 7.6.100.0 への移行が必要
7.2	N/A	7.4.121.0 または 7.6.100.0 への移行が必要
7.3	N/A	7.4.121.0 または 7.6.100.0 への移行が必要

* 4400/WiSM1/3750/2000コントローラは7.0コードを超えてアップグレードできない

CiscoワイヤレスLANコントローラのMLDv2におけるDoS脆弱性		
影響を受けるリリース	最初の修正	推奨
7.2	N/A	7.4.121.0 または 7.6.100.0 への移行が必要
7.3	N/A	7.4.121.0 または 7.6.100.0 への移行が必要
7.4	7.4.121.0	7.4.121.0 に移行
7.5	N/A	7.4.121.0 または 7.6.100.0 への移行が必要

CiscoワイヤレスLANコントローラにおける巧妙に細工されたフレームによるDoS脆弱性 CVE-2014-0706		
影響を受けるリリース	最初の修正	推奨
7.2	7.2.115.2	7.4.121.0 または 7.6.100.0 への移行が必要
7.3	N/A	7.4.121.0 または 7.6.100.0 への移行が必要
7.4	7.4.110.0	7.4.121.0

CiscoワイヤレスLANコントローラにおける巧妙に細工されたフレームによるDoS脆弱性 CVE-2014-0707		
影響を受けるリリース	最初の修正	推奨
7.2	N/A	7.4.121.0 または 7.6.100.0 への移行が必要
7.3	N/A	7.4.121.0 または 7.6.100.0 への移行が必要
7.4	7.4.110.0	7.4.121.0

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

Cisco Wireless LAN Controllerのサービス拒否の脆弱性、Cisco Wireless LAN ControllerのMLDv2のサービス拒否の脆弱性、およびCisco Wireless LAN Controllerの巧妙に細工されたフレームによるサービス拒否の脆弱性は、内部テスト中に発見されましたが、お客様の導入では見つかりませんでした。

Cisco Wireless LAN Controller Unauthorized Access to Associated Access Points Vulnerability、Cisco Wireless LAN Controller IGMPバージョン3サービス拒否の脆弱性、およびCisco Wireless LAN Controllerの巧妙に細工されたフレームによるサービス拒否の脆弱性は、お客様の問題の調査中にCisco TACによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140305-wlc

改訂履歴

リビジョン 1.0	2014年3月5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。