Ciscoワイヤレス LAN コントローラの多重 脆弱点

Critical

アドバイザリーID : cisco-sa-20130123-wlc
初公開日 : 2013-01-23 16:00
最終更新日 : 2013-01-30 20:36
バージョン 1.3 : Final
CVSSスコア : 9.0
回避策 : No Workarounds available
Cisco バグ ID : CSCtx80743 CSCua60653 CSCts87659 CSCuc15636

CVE-2013-1103
CVE-2013-1102
CVE-2013-1105
CVE-2013-1104

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ワイヤレス LAN コントローラ（Cisco WLC）製品 グループは次の 4 脆弱性から影響を受けます:

- Ciscoワイヤレス LAN コントローラ ワイヤレス Intrusion Prevention System （wIPS）サービス拒否の脆弱性
- Ciscoワイヤレス LAN コントローラ Session Initiation Protocol（SIP） サービス拒否の脆弱性
- リモート コード 実行脆弱性をプロファイルしている Ciscoワイヤレス LAN コントローラ HTTP
- Ciscoワイヤレス LAN コントローラ SNMP 不正アクセス脆弱性

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 これら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、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130123-wlc

該当製品

Cisco WLC 製品 グループは多重 脆弱点から影響を受けます。 Cisco WLC ソフトウェアの影響を受けたバージョンは特定の脆弱性によって変わります。

脆弱性のある製品

特定のバージョン情報に関しては、この状況報告のソフトウェア バージョン および 修正セクションを参照して下さい。
以下の製品のそれぞれはこの Security Advisory でカバーされる脆弱性の少なくとも 1 から影響を受けます:

- Cisco 2000 シリーズ WLC
- Cisco 2100 シリーズ WLC
- Cisco 2500 シリーズ WLC
- Cisco 4100 シリーズ WLC
- Cisco 4400 シリーズ WLC
- Cisco 5500 シリーズ WLC
- Cisco 7500 シリーズ WLC
- Cisco 8500 シリーズ WLC
- Cisco 500 シリーズ ワイヤレス Express モビリティ コントローラ
- Ciscoワイヤレス サービス モジュール（Cisco WiSM）
- Ciscoワイヤレス サービス モジュール バージョン 2（2）Cisco WiSM バージョン
- 統合サービス ルータ（ISR）のための Cisco NME-AIR-WLC モジュール
- 統合サービス ルータ（ISR）のための Cisco NM-AIR-WLC モジュール
- Cisco Catalyst 3750G 統合された WLCs
- Cisco Flex 7500 シリーズ Cloud コントローラ
- Cisco Virtual Wireless Controller
- Integrated services module 300 および Cisco Services-Ready Engine（SRE）モジュール 700、710、900、および 910 のための Ciscoワイヤレス コントローラ ソフトウェア

注: Cisco 2000 シリーズ WLCs は、Cisco 4100 シリーズ WLCs、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、終りのソフトウェア メンテナンスに達しました。 次のテーブルは各モデルのための廃止 文書 URL が含まれています:

モデル	ライフ文書 URL の終わり
Cisco 2000 シリーズ WLC	http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6308/prod_end-o
ISR のための Cisco NM-AIR-WLC モジュール	http://www.cisco.com/en/US/prod/collateral/modules/ps2797/prod_end-of-life_notice090
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

ある特定の環境で動作している Cisco WLC ソフトウェア バージョンを判別するために、次のいずれかの方式を使用して下さい:

Webインターフェイスで、 **Monitor タブを**選択し、左ペインの **要約を**クリックし、 **ソフトウェア バージョン** フィールドに注意して下さい。

コマンドラインインターフェイスでは、次の例に示すように **show sysinfo** コマンドを発行して下さい:

```
(Cisco Controller)> show sysinfo

Manufacturer's Name.. Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 5.1.151.0
RTOS Version..... Linux-2.6.10_mvl401
Bootloader Version... 4.0.207.0
Build Type..... DATA + WPS
<output suppressed>
```

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 WLCs および Cisco WiSMs はセキュリティポリシー、侵入防御、RF 管理、サービス品質（QoS）およびモビリティを含むシステム全体の Wireless LAN 機能に責任があります。 これらのデバイスはあらゆるレイヤ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および制御およびワイヤレスアクセスポイント（CAPWAP）プロトコルのプロビジョニング上のコントローラ ベースのアクセス ポイントと Lightweight Access Point Protocol（LWAPP）を使用して交信を行います。

デバイスの Cisco WLC 系列は次の脆弱性から影響を受けます:

Ciscoワイヤレス LAN コントローラ ワイヤレス Intrusion Prevention System（wIPS）サービス拒否の脆弱性

Ciscoワイヤレス LAN コントローラ（WLC）製品 グループにより非認証を可能にする可能性があるサービス拒否（DoS）脆弱性からリモート攻撃者 デバイスは影響を受けたデバイスへ巧妙に細工された IP パケットを送信 することによってリロードします影響を受けます。 この脆弱性は Cisco WLCs に影響を与えますワイヤレス Intrusion Prevention System（wIPS）で設定される。 この脆弱性は配線されたワイヤレス セグメントから不正利用することができます。

この脆弱性は Cisco バグ ID CSCtx80743 で（登録ユーザ専用）文書化されています、CVE ID CVE-2013-1102 を割り当てられました。

Ciscoワイヤレス LAN コントローラ Session Initiation Protocol（SIP）サービス拒否の脆弱性

AP を影響を受けたデバイスへ巧妙に細工された セッション開始プロトコル（SIP）パケットを送信 することによってリロードするために引き起こすために Ciscoワイヤレス Access Points（AP）で存在 する サービス拒否 （DoS）脆弱性非認証を許可する可能性がある Ciscoワイヤレス LAN コントローラ（WLC）によって管理されるリモート攻撃者。 この脆弱性は配線されたワイヤレス セグメントから不正利用することができます。

この脆弱性はトランジットトラフィックによって SIP 機能がデバイスでディセーブルにされても引き起こし。

この脆弱性は Cisco バグ ID CSCts87659（ 登録ユーザのみ）で文書化されています、CVE ID CVE-2013-1103 を割り当てられました。

リモート コード 実行脆弱性をプロファイルしている Ciscoワイヤレス LAN コントローラ HTTP

Cisco WLC デバイスの機能をプロファイルする HTTP は認証される可能にするかもしれないリモート コード 実行脆弱性からリモート攻撃者 UserAgent 巧妙に細工された ストリングの送信による影響を受けたデバイスの任意のコードを実行するために影響を受けます。 この脆弱性は配線されたワイヤレス セグメントから不正利用することができます。

Cisco WLC ソフトウェア バージョンだけ 7.3.101.0 この脆弱性から影響を受けます。 デバイスは機能をプロファイルする HTTP がイネーブルになっているときだけ脆弱です。

機能をプロファイルする HTTP がイネーブルになっていたかどうか確認するために、 **show wlan** コマンドを発行し、「ネットワーク アドミッション コントロール」「セクションの下で「HTTP」オプションを見つけて下さい。 次の例はイネーブルになっている機能を示したものです:

```
(WLC)>show wlan 3
WLAN Identifier.................................. 3
<output suppressed>
Network Admission Control
 Client Profiling Status ....................... Enabled
  DHCP ......................................... Disabled
  HTTP ......................................... Enabled
<output suppressed>
```

この脆弱性は Cisco バグ ID CSCuc15636（ 登録ユーザのみ）で文書化されています、CVE ID CVE-2013-1104 を割り当てられました。

Ciscoワイヤレス LAN コントローラ SNMP 不正アクセス脆弱性

Ciscoワイヤレス LAN コントローラ（WLC）製品 グループは認証された攻撃者が SNMP によって影響を受けた Cisco WLC の設定を表示し、修正する可能性がある不正アクセス脆弱性から「ワイヤレス」が機能上の管理無効でも影響を受けます。
この脆弱性は Cisco バグ ID CSCua60653（ 登録ユーザのみ）で文書化されています、CVE ID CVE-2013-1105 を割り当てられました。

回避策

以降のセクションはこの Security Advisory に説明がある各脆弱性のための回避策についての情報が、もし可能であれば、含まれています。

Ciscoワイヤレス LAN コントローラ ワイヤレス Intrusion Prevention System（wIPS）サービス拒否の脆弱性

Cisco WLC の wIPS 機能をディセーブルにすることのほかのこの脆弱性を軽減する回避策がありません。

Ciscoワイヤレス LAN コントローラ Session Initiation Protocol（SIP） サービス拒否の脆弱性

この脆弱性を軽減する回避策がありません。

リモート コード 実行脆弱性をプロファイルしている Ciscoワイヤレス LAN コントローラ HTTP

Cisco WLC の機能をプロファイルする HTTP をディセーブルにすることのほかのこの脆弱性を軽減する回避策がありません。

Ciscoワイヤレス LAN コントローラ SNMP 不正アクセス脆弱性

CPU によって基づくアクセス コントロール リスト（ACL）は影響を受けた WLC への SNMP アクセスを制限するために設定することができます。 ACL が定義された後、マネージメントインターフェイス、アクセス ポイント マネージャ（AP マネージャ）インターフェイス、またはクライアント データ トラフィックのための動的インターフェイスの何れかにまたはコントローラ CPU へのトラフィックのためのネットワーク演算処理装置（NPU）インターフェイスに適用することができます。

修正済みソフトウェア

次のテーブルはこの Security Advisory に説明がある脆弱性を軽減するためにソフトウェアアップグレード情報を提供します:

/ID	First Fixed Release	First Fixed Release
wIPS DoS CSCtx80743	4.2	

	4.2M	
	5.0	
	5.1	
	5.2	
	6.0	
	7.0	7.0.235.0
	7.1	; 7.2
	7.2	7.2.110.0
	7.3	7.3.101.0
	7.4	
SIP DoS CSCts87659	4.2	
	4.2M	
	5.0	
	5.1	
	5.2	
	6.0	
	7.0	7.0.220.0
	7.1	7.1.91.0
	7.2	7.2.103.0
	7.3	
	7.4	
HTTP CSCuc15636	4.2	
	4.2M	
	5.0	
	5.1	
	5.2	
	6.0	
	7.0	
	7.1	
	7.2	
	7.3	7.3.112.0
	7.4	
CSCua60653	4.2	

	4.2M	
	5.0	
	5.1	
	5.2	
	6.0	
	7.0	7.0.235.3
	7.1	; 7.2
	7.2	7.2.111.3
	7.3	7.3.101.0
	7.4	

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 Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける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。

推奨されるリリース

「推奨されるリリース」表はこの状況報告の時にすべての送達された脆弱性のための修正があるリリースをリストしたものです。 Cisco は「推奨されるリリース」表の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。

First Fixed Release	
7.0	7.0.235.3
7.1	; 7.2
7.2	7.2.111.3
7.3	7.3.112.0
7.4	

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不正利用事例とその公表は確認しておりません。

DoS およびリモート コード 実行脆弱性は弊社販売代理店要求のトラブルシューティングの間に発見されました。 SNMP 不正アクセス脆弱性は Darren ジョンソンCCIE#20078によって Cisco に発見され、報告されました。 Cisco PSIRT はセキュリティーの脆弱性の研究者とはたらく機会を非常に認め、製品レポートで検討し、助ける機会を歓迎します。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130123-wlc

改訂履歴

リビジョン 1.3	2013-January-30	ソフトウェア バージョン および 修正セクションの更新済表。
リビジョン 1.2	2013-January-24	ソフトウェア バージョン および 修正セクションの更新済表。
リビジョン 1.1	2013-January-23	SIP 脆弱性のための更新済詳細セクション。
リビジョン 1.0	2013-January-23	初回公開リリース

利用規約