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-20100908-wlc

初公開日 : 2010-09-08 16:00

バージョン 1.1 : Final

CVSSスコア : 9.0

回避策 : Yes

Cisco バグ ID :

CVE-2010-0574
CVE-2010-3034
CVE-2010-3033
CVE-2010-2843
CVE-2010-0575
CVE-2010-2842
CVE-2010-2841

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（WLC）製品 グループはこれらの脆弱性から影響を受けます :

- 2 サービス拒否 （DoS）脆弱性
- 3 特権 拡大脆弱性
- 2 Access Control List （ACL） バイパス の 脆弱性

注: これらの脆弱性は互いの依存しないです。 ある機器が 1 つの脆弱性の影響を受け、他の脆弱性の影響は受けない場合もあります。

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。

これらの脆弱性を軽減する回避策はありません。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100908-wlc で掲示されます。

該当製品

修正済みソフトウェア

これらの製品はそれぞれこの Security Advisory でカバーされる少なくとも 1 脆弱性から影響を受けます:

- Cisco 2000 シリーズ WLC
- Cisco 2100 シリーズ WLCs
- Cisco 4100 シリーズ WLCs
- Cisco 4400 シリーズ WLCs
- Cisco 5500 シリーズ WLCs
- Ciscoワイヤレス サービス モジュール（WiSMs）
- 統合サービス ルータ（ISR）のための Cisco WLC モジュール
- Cisco Catalyst 3750G 統合された WLCs

DoS 脆弱性

Cisco WLC 製品 グループは 2 DoS 脆弱性から影響を受けます:

- インターネット キー エクスチェンジ（IKE） DoS 脆弱性
- HTTP DoS 脆弱性

IKE DoS 脆弱性は Cisco WLC ソフトウェア バージョン 3.2 およびそれ以降に影響を与えます。 HTTP DoS 脆弱性は Cisco WLC ソフトウェア バージョン 4.2 と それ以降に影響を与えます。

特権 拡大脆弱性

特権 拡大脆弱性は Cisco WLC ソフトウェア バージョン 4.2 と それ以降に影響を与えます。

CPU ACL バイパス の 脆弱性

ACL バイパス の 脆弱性影響 Cisco 2 WLC ソフトウェア バージョン 4.1 と それ以降の 1 つ。第 2 ACL バイパス の 脆弱性は Cisco WLC ソフトウェア バージョン 6.0.x に影響を与えます。

ソフトウェア バージョンの判断

管理者は Cisco WLCs で（Web かコマンドラインインターフェイスを使用して）または Cisco WiSM で動作しているソフトウェア バージョンを判別するこれらの指示を使用できます（Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのコマンドを使用して）。

Ciscoワイヤレス コントローラ

ある特定の環境で動作している WLC バージョンを判別するために、これらのメソッドの 1 つを使用して下さい:

- 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。

注: ISR で Cisco WLC モジュールを使用する顧客はコマンド・ラインの次 の ステップを実行する前に **service-module wlan コントローラ *<slot/port>* session コマンドを**発行する必要があります。 統合された WLC モジュールによって Cisco Catalyst 3750G スイッチを使用する顧客はコマンド・ラインの次 の ステップを実行する前に**セッション *<Stack-Member-Number>* プロセッサを 1 つの session コマンド**発行する必要があります。

- コマンドラインインターフェイスから、型は **sysinfo を示し、**この例に示すように**製品 Version フィールドに**、注意します:

```
(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>
```

Cisco WiSMs

それらが WiSM を使用している場合**提示 wism モジュール *<module number>* コントローラを** Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータの **1 つの status コマンド**使用して下さい。 バージョン 5.1.151.0 を示すこの例で証明されたようにソフトウェア

バージョンに注意して下さい、:

```
Router# show wism module 3 controller 1 status

WiSM Controller 1 in Slot 3
Operational Status of the Controller
   : Oper-Up
Service VLAN
   : 192
Service Port
   : 10
Service Port Mac Address
   : 0011.92ff.8742
Service IP Address
   : 192.168.10.1
Management IP Address
   : 192.168.1.123
Software Version
   : 5.1.151.0
Port Channel Number
   : 288
Allowed vlan list
   : 30,40
Native VLAN ID
   : 40
WCP Keep Alive Missed
   : 0
```

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。

改訂履歴

リビジョン 1.1	2010-September-09	リリース 4.0 のための追加された情報。
リビジョン 1.0	2010-September-08	初回公開リリース

利用規約