

Ciscoワイヤレス LAN コントローラの多重脆弱点

Critical	アドバイザーID : cisco-sa-20090727-wlc	CVE-2009-1166
	初公開日 : 2009-07-27 16:00	CVE-2009-1165
	バージョン 1.1 : Final	CVE-2009-1164
	CVSSスコア : 10.0	CVE-2009-1167
	回避策 : Yes	
	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

多重脆弱点は Ciscoワイヤレス LAN コントローラ (WLC) プラットフォームにあります。この Security Advisory は次の脆弱性の詳細を概説します:

- 不正な HTTP または HTTPS 認証応答サービス拒否の脆弱性
- SSH 接続サービス拒否の脆弱性
- 巧妙に細工された HTTP または HTTPS 要求 サービス拒否の脆弱性
- 巧妙に細工された HTTP または HTTPS 要求 無許可の設定修正脆弱性

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。

このアドバイザーはで揭示されます:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090727-wlc>

該当製品

修正済みソフトウェア

Cisco 1500 シリーズ、2000 シリーズ、2100 シリーズ、4400 シリーズ、4100 シリーズ、4200 シリーズ、ワイヤレス サービス モジュール (WiSM)、統合サービス ルータのための

WLC モジュール、および Cisco Catalyst 3750G 統合ワイヤレス LAN コントローラは次の脆弱性の何れか一つ以上から影響を受けます:

- 不正な HTTP または HTTPS 認証応答サービス拒否の脆弱性はソフトウェア バージョン 3.2 およびそれ以降に影響を与えます。
- SSH 接続サービス拒否の脆弱性はソフトウェア バージョン 3.2 およびそれ以降に影響を与えます。
- 巧妙に細工された HTTP または HTTPS 要求 サービス拒否の脆弱性はソフトウェア バージョン 4.1 とそれ以降に影響を与えます。
- 巧妙に細工された HTTP または HTTPS 要求 無許可の設定修正脆弱性はソフトウェア バージョン 3.2 およびそれ以降に影響を与えます。

ソフトウェア バージョンの判断

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、次のいずれかのメソッドを使用して下さい:

- 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: で WLC モジュールを Integrated Services Router (ISR) モジュール使用する顧客は (ISR) 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 1/0 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、次の例に示すように**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>
```

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 Series/7600 シリーズ スイッチの 1 つの **status** コマンド使用して下さい。バージョン 5.1.151.0 を示す次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

Ciscoワイヤレス コントローラ 5500 シリーズはこれらの脆弱性から影響を受けません。

改訂履歴

リビジョン 1.1	2009- October-15	脆弱性が存在する製品 セクション および ソフトウェア バージョン および 修正 表の WLC リリース 3.2 についての追加された情報
リビジョン 1.0	2009-July- 27	初版リリース

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、単独の転載や意識を施した場合、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。