シスコ ワイヤレス LAN コントローラでのシンプル ネットワーク管理プロトコル メモリ リークにおけるサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20171101-wlc1

初公開日 : 2017-11-01 16:00

最終更新日 : 2017-11-02 18:35

バージョン 1.1 : Final

CVSSスコア : 7.7

回避策 : No workarounds available

Cisco バグ ID : CSCvc71674

CVE-2017-12278

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

シスコ ワイヤレス LAN コントローラの Simple Network Management Protocol（SNMP）サブシステムにおける脆弱性により、認証を受けているリモート攻撃者が該当デバイスの再起動を引き起こし、その結果、サービス妨害（DoS）状態が発生する可能性があります。

この脆弱性は、特定の MIB のポーリングに使用されるバッファの割り当て解除を該当デバイスが失敗した後に同デバイスで発生するメモリ リークに起因するものです。 SNMPv2 *SNMP* を知っている攻撃者はストリングを *読むか*、または影響を受けたデバイスのための有効な SNMP バージョン 3 資格情報が繰り返し影響を受けた MIBオブジェクトID（OID）をポーリングし、デバイスの利用可能なメモリを消費する可能性がありますあります。 デバイスのメモリが大量に消費されると、デバイスが再起動して、DoS 状態に至ります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
101-wlc1

該当製品

脆弱性のある製品

この脆弱性は、SNMP が有効になっており、なおかつ脆弱なリリースのシスコ ワイヤレス LAN コントローラ（WLC）ソフトウェアを実行している Cisco WLC に影響します。

情報に関しては Cisco どのについての WLC ソフトウェア リリースが脆弱であるか、このアドバイザリの修正済みソフトウェアのセクションを参照して下さい。

SNMP 設定の検証

SNMP がデバイスで有効に なるかどうか判別するために、管理者は CLI の**提示実行構成**コマンドを発行できます。 **config snmp *<1/2/3>* enable コマンドは**実行コンフィギュレーションにあることをコマンドの出力が示したもので、SNMP はデバイスで有効に なります。

Cisco WLC ソフトウェア リリースの判別

デバイスで実行されている Cisco WLC ソフトウェアのリリースを確認するには、管理者は Web インターフェイスか CLI を使用します。

Web インターフェイスを使用する場合は、Web インターフェイスにログインして **Monitor** タブをクリックし、次に左ペインの **Summary** をクリックします。 **ソフトウェア バージョン** フィールドはデバイスで現在動作しているソフトウェアのリリース番号を示します。

CLI を使用する場合は、**show sysinfo** コマンドを実行し、次にコマンド出力の **Product Version** フィールドの値を参照して下さい。 たとえばデバイスが Cisco WLC ソフトウェア リリース 8.3.102.0 を実行している場合、コマンドの出力は次のようになります。

```
(wlc)> show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.3.102.0
Bootloader Version............................... 1.0.1
Field Recovery Image Version..................... 6.0.182.0
Firmware Version................................. FPGA 1.3, Env 1.6, USB console 1.27
Build Type....................................... DATA + WPS
.
.
.
```

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

セキュリティ侵害の痕跡

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

カスタマーは、このセクションの表に沿って、適切なリリースへのアップグレードをおこなってください。 本アドバイザリは以下のアドバイザリを含むコレクションの一部です。これらも考慮した上、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。

- cisco-sa-20171101-aironet1: Cisco Aironet 1560、2800、および 3800 シリーズ アクセス ポイント プラットフォームでの 802.11 におけるサービス妨害（DoS）の脆弱性
- cisco-sa-20171101-aironet2: Cisco Aironet 1560、2800、および 3800 シリーズ アクセス ポイント プラットフォームでの Extensible Authentication Protocol におけるサービス妨害（DoS）の脆弱性
- cisco-sa-20171101-wlc1: シスコ ワイヤレス LAN コントローラでのシンプル ネットワーク管理プロトコル メモリ リークにおけるサービス妨害（DoS）の脆弱性
- cisco-sa-20171101-wlc2: シスコ ワイヤレス LAN コントローラでの 802.11v Basic Service Set 移行管理におけるサービス妨害（DoS）の脆弱性

次の表では、左の列にシスコ ソフトウェアのリリースを示しています。 中央の列は、この脆弱性の修正が含まれた最初の推奨リリースです。 右の列は、このアドバイザリ集で説明しているすべての脆弱性の修正が含まれた最初の推奨リリースです。

Cisco Wireless LAN Controller ソフトウェア リリース	この脆弱性のための推奨される修正済みリリース	アドバイザリの収集に説明
Prior to 8.0	8.0.152.0	8.0.152.0
8.0	8.0.152.0	8.0.152.0
8.1	8.2.166.0	8.2.166.0
8.2	8.2.166.0	8.2.166.0
8.3	8.3.133.0	8.3.133.0
8.4	8.4.100.0	8.4.100.0
8.5	8.5.110.0（リリース予定）	8.5.110.0（リリース予定）

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やその公表を確認していません。

出典

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-wlc1

改訂履歴

Version	Description	Section	Status	日付
1.1	WLC リリース 8.2 と 8.3 は、お客様の問題に対処するために再ビルドされました。 推奨リリースが更新されました。	修正済みソフトウェア	Final	2017 年 11 月 2 日
1.0	初回公開リリース		Final	2017 年

				11 月 1 日

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、単独の転載や意訳を施した場合、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。