Cisco Policy Suite の RADIUS 認証バイパスの脆弱性

High

アドバイザリーID : cisco-sa-20180207-cps
初公開日 : 2018-02-07 16:00
バージョン 1.0 : Final
CVSSスコア : 7.2
回避策 : No workarounds available
Cisco バグ ID : CSCvg40124

CVE-2018-0116

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 Policy Suite の RADIUS 認証モジュールにおける脆弱性により、認証されていないリモート攻撃者が、有効なパスワードを指定せずにサブスクライバとして承認される可能性があります。 ただし、攻撃者は有効なユーザ名を指定する必要があります。

この脆弱性は、RADIUS でユーザ クレデンシャルが正しく確認されていないことに起因しています。 攻撃者は、RADIUS 認証が設定された Cisco Policy Suite ドメインにアクセスしてこの脆弱性をエクスプロイトする可能性があります。 エクスプロイトに成功すると、有効なパスワードを指定せずにサブスクライバとして承認される可能性があります。

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。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-cps

該当製品

脆弱性のある製品

この脆弱性は、RADIUS 認証がドメインに設定されている場合に、Cisco Policy Suite のリリース 13.1.0 ホットフィックス パッチ 1 より前のリリースが実行されているアプリケーションに影響を及ぼします。 Cisco Policy Suite リリース 14.0.0 にも脆弱性が存在するため影響がありますが、RADIUS 認証は、Cisco Policy Suite リリース 14.0.0 以降では正式にはサポートされ

ていません。 影響を受けるソフトウェア バージョンの詳細については、本アドバイザリの「修正済みソフトウェア」セクションを参照してください。

アプリケーションで実行されているソフトウェア バージョンを確認する場合は、CLI から管理者権限で **about.sh** コマンドを実行します。 デバイスでソフトウェア リリース 12.1.0 が実行されている場合、次の例のようになります。

```
# about.sh
Cisco Policy Suite - Copyright (c) 2015. All rights reserved.
CPS Multi-Node Environment
CPS Installer Version - 12.1.0
.
.
.
CPS Patch History
--------------------------
No patches have been applied
.
.
.
```

ドメインでの認証に RADIUS を使用する場合にのみシステムに脆弱性が発生します。 RADIUS 認証はデフォルトでは有効にされていません。 管理者は、Policy Builder の GUI を使用して [サービス (Services)] タブにアクセスし、[ドメイン (Domains)] タブで該当のドメインを選択することで、そのドメインに RADIUS 認証が設定されているかどうかを確認できます。 [全般 (General)] タブで [USuM 承認 (USuM Authorization)] が選択され、[ユーザ ID (User Id)] フィールドと [パスワード (Password)] フィールドに **RADIUS のユーザ名**と**パスワード**がそれぞれ入力されているかどうかを確認します。

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。

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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.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。
https://www.cisco.com/c/en/us/support/web/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

次の表では、左の列に Cisco Policy Suite ソフトウェアのメジャー リリースを示します。 右の列は、メジャー リリースが本アドバイザリに記載している脆弱性に該当するかどうか、また、本脆弱性に対する修正を含む最初のマイナー リリースに該当するかどうかを示します。

次の表に示すように、適切なリリースにアップグレードする必要があります。

Cisco Policy Suite メジャー リリース	この脆弱性に対する最初の修正リリース
12.x より前	Vulnerable. 13.1.0 にアップグレードし、ホットフィックス パッチ 1 を適用します。
12.x	Vulnerable. 13.1.0 にアップグレードし、ホットフィックス パッチ 1 を適用します。
13.0	Vulnerable. 13.1.0 にアップグレードし、ホットフィックス パッチ 1 を適用します。
13.1	Vulnerable. ホットフィックス パッチ 1 を適用します。

14.0	Vulnerable. [1]
18.0	脆弱性なし

[1] Cisco Policy Suite リリース 14.0 には脆弱なコードが含まれていますが、正式には RADIUS 認証をサポートしていません。 後続の Cisco Policy Suite リリース 18.0 は RADIUS 認証をサポートしておらず、脆弱なコードは含まれていません。

Cisco Policy Suite 13.1.0 ホットフィックス パッチ 1 およびその他の Cisco Policy Suite ソフトウェアは、Cisco.com の Software Center でダウンロードできます。[ダウンロード ホーム（Downloads Home）] > [製品（Products）] > [ワイヤレス（Wireless）] > [モバイルインターネット（Mobile Internet）] > [サービスプロバイダー向けPolicy Suite（Policy Suite for Service Providers）] > [Policy Suite for Wi-Fi] > [Cisco Policy Suite（CPS）ソフトウェア（Cisco Policy Suite (CPS) Software）] の順に選択してください。

Cisco Policy Suite リリース 13.1.0 にホットフィックス パッチ 1 を適用する場合は、『CPS Migration and Upgrade Guide, Release 13.1.0（CPS の移行およびアップグレード ガイド リリース 13.1.0）』の「*Apply a Patch（パッチ適用）*」セクションを参照してください。

ホットフィックス パッチ 1 が適用されていることを確認する場合は、CLI から管理者権限で **about.sh** コマンドを実行してください。 次の例では、 **about.sh** コマンドの実行結果からパッチがすでに適用済みであることを確認できます。

```
# about.sh
Cisco Policy Suite - Copyright (c) 2015. All rights reserved.
CPS Multi-Node Environment
CPS Installer Version - 13.1.0
CPS Core Versions
---------------------------
hostname: qns-1 (pcrf): 13.1.1.r113649
hostname: qns-2 (pb): 13.1.1.r113649
.
.
.
CPS Patch History
---------------------------
CPS_Hotfix_Patch1_13.1.0
.
.
.
```

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

この脆弱性は、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-cps

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-February-07

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。