Cisco IOS XE ソフトウェア TrustSec によって保護されるアクセス クレデンシャル プロビジョニング サービス拒否の脆弱性

Medium	**アドバイザリーID :** cisco-sa-20190925-ctspac-dos **初公開日 :** 2019-09-25 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.8 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvo79239	CVE-2019-12663

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 IOS XE ソフトウェアの Cisco TrustSec （ CTS ）保護されたアクセス クレデンシャル （ PAC ）提供モジュールの脆弱性は引き起こすように非認証により、リモート攻撃者 サービス拒否 （ DoS ）状態に終って影響を受けたデバイスのリロードをする、可能性があります。

脆弱性は RADIUS メッセージの属性の不適当な検証が原因です。 攻撃者は影響を受けたデバイスへ悪意のある RADIUS メッセージを送信 することによってデバイスが特定の状態にある間、この脆弱性を不正利用する可能性があります。
シスコはこの脆弱性に対処するソフトウェア アップデートをリリースしました。 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-20190925-ctspac-dos

該当製品

脆弱性のある製品

パブリケーションの時に、この脆弱性は有効に なった CTS PAC 提供機能と Cisco IOS XE ソフトウェアの脆弱なリリースを実行していた Ciscoデバイスに影響を与えました。

詳細についてはどのに関する Cisco IOS XE ソフトウェアがリリースするかパブリケーションの時に脆弱、見ます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でした。

CTS PAC プロビジョニングが有効に なるかどうか判別して下さい

CTS PAC プロビジョニングが有効に なるかどうか判別するために、顧客は**提示 cts pacs** CLI コマンドを使用できます。 次の例は有効に なる CTS PAC プロビジョニングがあるデバイスの**提示 cts pacs** コマンドの出力を示したものです:

```
Switch# show cts pacs

AID: 1100E046659D4275B644BF946EFA49CD
PAC-Info:
PAC-type = Cisco Trustsec
.
.
.
```

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

シスコは、この脆弱性が Cisco IOS ソフトウェア、Cisco IOS XR ソフトウェア、および Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

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

影響を受けたおよび修正済みソフトウェアリリースについての詳細な情報に関しては、Cisco IOSソフトウェア チェッカーを参照して下さい。

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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。

Cisco IOS および IOS XE ソフトウェア

Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるよう、シスコでは Cisco IOS Software Checker ツールを提供しています。このツールにより、特定のソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。 また該当する場合、そのリリースに関するすべてのアドバイザリの脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用して次のタスクを実行できます。

- ドロップダウン リストからリリース（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- **show version** コマンドの出力をツールで解析する
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

リリースが、公開されたシスコ セキュリティ アドバイザリのいずれかに該当するかどうかを確認するには、Cisco.com の Cisco IOS Software Checker を使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェア リリース（たとえば、**15.1(4)M2**、**3.13.8S** など）を入力します。

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[Impact Rating] ドロップダウン リストの [中間（Medium）] チェックボックスをオンにします。

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-20190925-ctspac-dos

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019-September-25

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。