

Cisco IOSおよびIOS XEソフトウェアのTclにおけるサービス妨害(DoS)の脆弱性



アドバイザーID : cisco-sa-tcl-dos-

MAZQUnMF

初公開日 : 2020-06-03 16:00

最終更新日 : 2020-06-08 20:41

バージョン 1.1 : Final

CVSSスコア : [6.5](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvq28110](#)

[CVE-2020-3201](#)

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ソフトウェアおよびCisco IOS XEソフトウェアのTool Command Language(TCL)インタープリタにおける脆弱性により、認証された非特権のローカル攻撃者が、該当システムにサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、Tclインタープリタに渡されるデータの不十分な入力検証に起因します。攻撃者は、該当デバイスで巧妙に細工されたTcl引数を実行することにより、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は該当デバイスのリロードを引き起こし、その結果DoS状態が発生する可能性があります。

注 : デフォルトでは、Tclシェルアクセスには特権レベル15が必要です。カスタム権限の設定により、権限の低いユーザにTclシェルアクセスを許可できます。CVSSスコアはこれを考慮していません。

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。

このアドバイザーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tcl-dos-MAZQUnMF>

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOSソフトウェアまたはIOS XEソフトウェアの脆弱性が存在するリリースを実行しているシスコデバイスに影響を与えます。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

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[脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。](#)

シスコは、この脆弱性が Cisco IOS XR ソフトウェアまたは 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

[ソフトウェアのアップグレードを検討する](#)際には、[シスコのセキュリティアドバイザリおよびアラート (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。

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 Software Checker 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。

お客様は、[Cisco Software Checker を使用して次の方法でアドバイザリを検索できます。](#)

- ソフトウェアと 1 つ以上のリリースを選択します。
- 特定のリリースのリストを含む .txt ファイルをアップロードする
- show version コマンドの出力を入力する

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリ、特定のアドバイザリ、または最新の公開資料に記載されているすべてのアドバイザリが含まれるように検索をカスタマイズできます。

また、次のフォームで15.1(4)M2や3.13.8SなどのCisco IOSソフトウェアリリースまたはIOS XEソフトウェアリリースを入力して、そのリリースがCisco Security Advisoryのいずれかに該当するかどうかを確認することもできます。

<input type="text"/>	<input type="button" value="Check"/>
----------------------	--------------------------------------

デフォルトでは、[Cisco Software Checker の結果には、Security Impact Rating \(SIR \) が「重大」または「高」の脆弱性だけが含まれます。](#)「中間」の SIR 脆弱性の結果を含めるには、Cisco.com にある Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価 (Impact Rating)] の下にある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。

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、Cisco IOS XE ソフトウェアのリリースに応じて「[Cisco IOS XE 2 Release Notes](#)」、「[Cisco IOS XE 3S Release Notes](#)」、または「[Cisco IOS XE 3SG Release Notes](#)」を参照してください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tcl-dos-MAZQUnMF>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	必要な権限レベルを変更して低く設定し、この変更を反映するために概要セクションを更新。	CVSSスコアと概要	Final	2020年6月8日
1.0	初回公開リリース	—	Final	2020年6月3日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。