Cisco IOS XE ソフトウェア診断シェル パス走査脆弱性

Medium	**アドバイザリーID :** cisco-sa-20180207-ios **初公開日 :** 2018-02-07 16:00 **最終更新日 :** 2018-02-12 13:57 **バージョン 1.1 :** Final **CVSSスコア :** 4.4 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvg41950	CVE-2018-0123

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 ソフトウェアのための診断シェルの脆弱性はシステム ファイルを上書きできるある特定の診断 shell コマンドを使用する認証された、ローカル攻撃者を可能にする可能性があります。 これらのシステム ファイルは敏感かもしれ、診断シェルのユーザによって上書きできないはずです。

脆弱性はある特定の診断 shell コマンドのための適切な入力検証の欠けて当然です。 攻撃者はデバイスに認証し、診断シェルを入力し、ローカル診断シェル CLI でコマンドへ巧妙に細工されたユーザインプットを提供することによってこの脆弱性を不正利用する可能性があります。 不正利用の成功は攻撃者が制限されるはずであるシステム ファイルを上書きすることを可能にする可能性があります。

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-ios

該当製品

脆弱性のある製品

この脆弱性は Cisco IOS XE ソフトウェアに影響を与えます。 該当するソフトウェア リリースについての情報に関しては、この状況報告の上で Cisco バグ ID を参照して下さい。

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

修正済みソフトウェア リリースの詳細については、本アドバイザリ上部の Cisco Bug ID を参照ください。

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。

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

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

改訂履歴

Version	Description	Section	Status	日付
1.1	影響を受けた製品として Cisco IOS を参照する取除かれた不正確なテキスト。 Cisco IOS はこの脆弱性から影響を受けません。	説明、影響を受けたソフトウェア。	Final	2018-February-12
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。