Cisco Wide Area Application Services（WAAS）アプライアンス ソフトウェア ディスク チェック ツール特権 拡大脆弱性

Medium	**アドバイザリーID：** cisco-sa-20180606-waas-priv-escalation **初公開日：** 2018-06-06 16:00 **バージョン 1.0：** Final **CVSSスコア：** 6.7 **回避策：** No workarounds available **Cisco バグ ID：** CSCvi72673	CVE-2018-0352

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 Wide Area Application Services（WAAS）のためのディスク チェック ツール（*disk-check.sh*）の脆弱性は*定着するために*特権レベルを上げる認証された、ローカル攻撃者を可能にする可能性があります。 攻撃者はスーパ ユーザ特権の有効なユーザ 資格情報がなりません（デバイスにログインに 15）水平なければ。

脆弱性はディスク チェック ツールという点において実行されるスクリプトファイルの不十分な有効性確認が原因です。 攻撃者は悪意のあるスクリプト ファイルと 1 つのスクリプトファイルを置き換えることによって影響を受けたツールが動作している間この脆弱性を不正利用する可能性があります。 不正利用に成功すると、攻撃者は*ルート レベル*の権限を取得し、デバイスを完全に制御できるようになります。

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-20180606-waas-priv-escalation

該当製品

脆弱性のある製品

この脆弱性は Cisco Wide Area Application Services（WAAS）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、このアドバイザリの上で 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

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。

詳細

WAAS ディスク チェック ツール *（ディスクcheck.sh ）は* Cisco.com から取除かれなく、もはやダウンロード可能です。 ただし、まだツールがツールを以前にダウンロードした攻撃者によってまだこの脆弱性のための修正があっていない実行するデバイス WAAS ソフトウェアの特権を上げるのに使用できます。

この脆弱性のための修正はかなり WAAS ソフトウェアのスクリプト署名および有効性確認方法論を変更します。 この変更の結果として、前のメソッドを使用して署名したどのスクリプトでも WAAS リリースでもはや動作しませんこの脆弱性のための修正が含まれている。

署名されたスクリプトは一般的に リリースだけの設定 される限られたののための特定の問題を提起するために提供されます従ってまだ一般に以前のスクリプトがアップグレードの後で必要となると期待しません。 Cisco Technical Assistance Center （TAC）に接触するようにスクリプトをアップデートされて得るためにこの脆弱性を当たるリリースへのアップグレードが顧客助言された後それらがまだ適用する状況。

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

Cisco はこの脆弱性を報告するためにブリスベーンの暴動ソリューションからの外部研究者に、オーストラリア感謝することをアーロン ブレア望みます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-waas-priv-escalation

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-June-06

利用規約