Cisco Wide Area Application Services（WAAS）アプライアンス TCP フラグメント サービス拒否の脆弱性

Medium	**アドバイザリーID :** cisco-sa-20170621-waas	CVE-2017-6721
	送達される : 2017-06-21 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 5.8	
	回避策 : Yes	
	Cisco バグ ID : CSCvc57428	

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

フラグメント化された TCP パケットの入力処理の脆弱性はによる Cisco Wide Area Application Services（WAAS）アプライアンス（WAAS）非認証により、リモート攻撃者 WAASNET プロセスは予想に反して再起動しますする可能性がありまサービス拒否 （DoS）状態を引き起こします。

脆弱性はパケット チェーンがフラグメント化するとき TCP パケットの不完全な入力の検証が原因です。 攻撃者は影響を受けたデバイスを通して巧妙に細工された一組の TCP フラグメントの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により予想に反して再起動するプロセスによる DoS 状態を引き起こすことを可能にする可能性があります。 WAAS は WAASNET プロセスが再起動している短時間の間にトラフィックを廃棄する可能性があります。

この脆弱性に対処する回避策がありません。

621-waas

影響を受ける製品

脆弱性が存在する製品

この脆弱性は Cisco Wide Area Application Services（WAAS）アプライアンス影響を与えます

（WAAS）。 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。

脆弱性が存在しない製品

この脆弱性に影響されるその他のシスコ製品は現在のところ見つかっていません。

細部

回避策

この脆弱性に対処する回避策がありません。

固定ソフトウェア

修正済み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。

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、顧客はアップグレードされるべきデバイスが十分なメモリが含まれ、現在のハードウェア および ソフトウェア構成が新しいリリースによってきちんとサポートされ続けることを確認するようにする必要があります。 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製品 のセキュリティ上の問題に対する回答チーム（PSIRT）はこのアドバイザリに説明がある脆弱性の公示か不正利用に気づいていません。

ソース

この脆弱性は内部 保全テストの間に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-waas

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース		FINAL	2017-June-21

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。