Cisco適応型セキュリティアプライアンスCXコンテキスト認識型セキュリティサービス妨害(DoS)の脆弱性

High

アドバイザリーID : cisco-sa-20170125-cas

初公開日 : 2017-01-25 16:00

バージョン 1.0 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCva62946

CVE-2016-9225

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

適応型セキュリティアプライアンス(ASA)CXコンテキスト認識型セキュリティモジュールのデータプレーンIPフラグメントハンドラの脆弱性により、認証されていないリモートの攻撃者がCXモジュールをそれ以上のトラフィックを処理できなくなり、その結果サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、IPフラグメントの不適切な処理に起因します。攻撃者は、巧妙に細工されたフラグメント化されたIPトラフィックをCXモジュールに送信することで、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、攻撃者は共有メモリ(SHM)内の空きパケットバッファを使い果たし、CXモジュールがそれ以上のトラフィックを処理できなくなり、その結果DoS状態が発生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ておらず、リリースする予定もありません。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170125-cas

該当製品

脆弱性のある製品

この脆弱性は、ASA CX Context-Aware Securityモジュールのすべてのバージョンに影響します。

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。

詳細

Cisco ASA CX Context-Aware Securityモジュールは、ASAプラットフォームを拡張するアドオンサービスモジュールで、コンテキスト認識機能を使用して可視性と制御を強化します。

親Cisco ASAのモジュラポリシーフレームワーク(MPF)設定によってCisco ASA CXに向けられたユーザトラフィックのみが、このアドバイザリに記載されている脆弱性の影響を受けます。

回避策

この脆弱性に対処する回避策はありません。次の緩和策は、この脆弱性の発現を制限するのに役立ちます。

次のように、受信したIPフラグメントをドロップするようにASAを設定します。

```
ASA# conf t
ASA(config)# fragment chain 1
ASA(config)# exit
```

注意：この設定はグローバルにのみ行うことができるため、Cisco ASA CXモジュールに特に向けられたトラフィックだけでなく、ASAを通過するすべてのユーザトラフィックに影響が及ぶことに注意してください。この設定では、このトラフィックがASA CXモジュールで処理されなくても、すべてのIPフラグメントがASAによって廃棄されます。

修正済みソフトウェア

シスコはこのアドバイザリに記載された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おらず、リリースする予定もありません。ASA CXモジュールは、サポート終了(EoL)プロセスに入りました。この製品のEoL通知を参照してください。
Cisco ASA CX Context-Aware SecurityおよびCisco Prime Security Managerの販売終了およびサポート終了のお知らせ
Cisco ASA with FirePOWER Servicesへの移行をお勧めします。

デバイスの移行を検討する際は、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、お客様は新しいデバイスがネットワークのニーズに十分に対応できることを確認する必要があります。新しいデバイスには十分なメモリが搭載され、現在のハードウェアおよ

びソフトウェア構成は新しい製品でも引き続き適切にサポートされます。情報が明確でない場合は、シスコアカウントチームの担当者またはシスコパートナ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）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

この問題は、カスタマーサポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170125-cas

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	初回公開リリース	-	Final	2017 年 1 月 25 日

利用規約

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。