

Cisco FirePOWER Malware Protectionバイパスの脆弱性

Medium	アドバイザーID : cisco-sa-20161207-fpwr	CVE-2016-9209
	初公開日 : 2016-12-07 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 4.3	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvb20102	

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 FirePOWERシステムソフトウェアのTCP処理における脆弱性により、認証されていないリモートの攻撃者が、通常はブロックされるファイルをダウンロードできる可能性があります。

この脆弱性は、HTTPインスペクションに渡される前にTCPセグメント（確認応答済みの現在のウィンドウからの再送信）が正しく処理されないことに起因します。GZIP圧縮ストリームでは、GZIPの圧縮解除が失敗します。この結果、不正なSHA-256ハッシュが計算され、潜在的なマルウェアが検出されません。攻撃者は、この脆弱性を不正利用して、特別に準備されたサーバからHTTP経由でマルウェアを含むファイルをダウンロードするようにユーザを誘導する可能性があります。この不正利用により、攻撃者はFirePOWERシステムソフトウェアによって提供されるマルウェア防御をバイパスでき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で確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-fpwr>

該当製品

脆弱性のある製品

次のシスコ製品に脆弱性が存在します。

- FirePOWER サービスを使用する適応型セキュリティ アプライアンス (ASA) 5500-X シ

リーズ

- ネットワーク向け Advanced Malware Protection (AMP) 7000 シリーズ アプライアンス
- ネットワーク向け Advanced Malware Protection (AMP) 8000 シリーズ アプライアンス
- FirePOWER 7000 シリーズ アプライアンス
- FirePOWER 8000 シリーズ アプライアンス
- サービス統合型ルータ (ISR) 向け FirePOWER Threat Defense
- Blue Coat Xシリーズ向け次世代侵入防御システム(NGIPS)
- Sourcefire 3D システム アプライアンス
- VMware 向け仮想次世代侵入防御システム (NGIPSv)

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は、[Cisco Security Advisories and Alertsページ](#)から入手できるシスコ製品のアドバイザリを参照して、侵害の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) 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

この脆弱性はサポート ケースの解決中に発見されました。

URL

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	2016年11月28日

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。