

# Cisco Firepower システム ソフトウェア サーバ メッセージ ブロック バージョン 2 ファイル ポ リシー バイパスの脆弱性

<b>Mediu m</b>	アドバイザーID : cisco-sa- 20171115-firepower2	<a href="#">CVE- 2017- 12300</a>
	初公開日 : 2017-11-15 16:00 バージョン 1.0 : Final CVSSスコア : <a href="#">5.8</a> 回避策 : No workarounds available Cisco バグ ID : <a href="#">CSCve58398</a>	

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 ソフトウェアの検出エンジンの脆弱性はサーバ メッセージ ブロック バージョン 2 ( SMB2 ) プロトコルをブロックするために設定されるリモート攻撃者非認証がファイル ポリシーをバイパスするようにする可能性があります。

脆弱性は検出がファイルの長さに基づいているとき SMB2 ファイルの不正確な検出が原因です。攻撃者は目標とされたデバイスを通して巧妙に細工された SMB2 Transfer 要求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。正常なエクスプロイトは攻撃者が SMB2 トラフィックをブロックするために設定されるフィルターをバイパス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。

このアドバイザーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-firepower2>

## 該当製品

### 脆弱性のある製品

この脆弱性は影響を与えます Cisco Firepower システム ソフトウェアに- SNORT は影響を受けています。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 TAC のサポート案件の対応時に発見されました。

### URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-firepower2>

### 改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017 年 11 月 15 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。

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。