Cisco Firepower Threat Defense ソフトウェアの SMB プロトコル プリプロセッサ検出エンジンにおけるサービス妨害（DoS）の脆弱性

アドバイザリーID : cisco-sa-20190501-frpwr-smb-snort
初公開日 : 2019-05-01 16:00
最終更新日 : 2019-05-02 17:54
バージョン 1.1 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCvj83264 CSCvj91418

CVE-2019-1704
CVE-2019-1696

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 Threat Defense（FTD）ソフトウェアのサーバ メッセージ ブロック（SMB）プロトコル プリプロセッサ検出エンジンに存在する複数の脆弱性により、認証されていない隣接またはリモートの攻撃者がサービス妨害（DoS）状態を引き起こせる危険性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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います。これら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-20190501-frpwr-smb-snort

該当製品

脆弱性のある製品

これらの脆弱性は、Cisco FTD ソフトウェアの脆弱性が存在するリリースを実行する次のシスコ製品に影響を与えます。

- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）

- 適応型セキュリティ アプライアンス（ASA）5500-X シリーズ ファイアウォール
- ASA 5500-X with FirePOWER Services シリーズ
- FirePOWER 7000 シリーズ アプライアンス向け Advanced Malware Protection（AMP）for Networks
- FirePOWER 8000 シリーズ アプライアンス向け AMP for Networks
- Firepower 2100 シリーズ
- Firepower 4100 シリーズ
- 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
- Firepower 9300 セキュリティ アプライアンス
- サービス統合型ルータ（ISR）向け FirePOWER Threat Defense
- FTD Virtual（FTDv）
- 次世代侵入防御システム（NGIPS）

脆弱性が存在する Cisco FTD ソフトウェア リリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

これらの脆弱性は、オープンソースの Snort プロジェクトにも影響を与える可能性があります。詳細については、Snort の Web サイトを参照してください。

Cisco FTD ソフトウェア リリースの判別

デバイスで実行中の Cisco FTD ソフトウェア リリースを確認するために、管理者はデバイスにログインし、CLI で show version コマンドを使用してコマンドの出力を参照できます。デバイスが Cisco FTD ソフトウェア リリース 6.2.0 を実行している場合、コマンドの出力例は次のようになります。

```
<#root>

>

show version


--------------------[ ftd ]---------------------
Model : Cisco ASA5525-X Threat Defense (75) Version 6.2.0 (Build 362)
UUID : 2849ba3c-ecb8-11e6-98ca-b9fc2975893c
Rules update version : 2017-03-15-001-vrt
VDB version : 279
-----------------------------------------------------
```

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、これらの脆弱性の影響を受けることが分かっています。

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Firepower Management Center
- Meraki MX セキュリティ アプライアンス

詳細

Cisco FTD ソフトウェアの SMB プロトコル プリプロセッサ検出エンジンに存在する 2 つの脆弱性により、隣接またはリモートの攻撃者が DoS 状態を引き起こせる危険性があります。

これらの脆弱性は互いに依存していないため、一方の脆弱性を悪用しても他方の脆弱性を悪用する必要はありません。

これらの脆弱性の詳細については、次のとおりです。

Cisco Firepower Threat Defense ソフトウェアの SMB プロトコル プリプロセッサ検出エンジンにおける低システム メモリ サービス妨害の脆弱性

Cisco FTD ソフトウェアの SMB プロトコル プリプロセッサ検出エンジンの脆弱性により、認証されていない隣接の攻撃者がデバイスのシステム メモリを不足させ、デバイスからのトラフィックの転送が停止する危険性があります。この状態を解消するために手動でのデバイスのリロードが必要になることがあります。

この脆弱性は、特定の SMB パケット タイプに対する SMB 入力パケットの処理が正しく行われないことに起因します。攻撃者は、ローカル サブネットからターゲット デバイスに細工された SMB パケットの一定のストリームを送信することにより、この脆弱性をエクスプロイトする危険性があります。エクスプロイトが成功すると、攻撃者がデバイスのシステム メモリを不足させ、Snort プロセスにおけるトラフィックの転送が阻止される危険性があります。この脆弱性は、IPv4 か IPv6 と SMB バージョン 2（SMBv2）または SMB バージョン 3（SMBv3）のネットワーク トラフィックのいずれかを組み合わせて使用することでエクスプロイトできます。

この脆弱性のCommon Vulnerabilities and Exposures(CVE)IDはCVE-2019-1696です。

この脆弱性のSecurity Impact Rating(SIR)はHighです。

Cisco Firepower Threat Defense ソフトウェアの SMB プロトコル プリプロセッサ検出エンジンにおけるサービス妨害の脆弱性

Cisco FTD ソフトウェアの SMB プロトコル プリプロセッサ検出エンジンの脆弱性により、認証されていないリモートの攻撃者が Snort プロセスを突然再起動させ、サービス妨害（DoS）状態が発生する危険性があります。

この脆弱性は、特定の SMB パケット タイプに対する SMB 入力パケットの処理が正しく行われないことに起因します。攻撃者は、ターゲット デバイスに細工された SMB 接続を送信すること

により、この脆弱性をエクスプロイトする危険性があります。エクスプロイトが成功すると、攻撃者が Snort プロセスをクラッシュさせることができる危険性があります。この脆弱性は、IPv4 か IPv6 と SMBv2 または SMBv3 のネットワーク トラフィックのいずれかを組み合わせて使用することでエクスプロイトできます。

この脆弱性のCVE IDはCVE-2019-1704です。

この脆弱性のSIRはHighです。

セキュリティ侵害の痕跡

Cisco Firepower Threat Defense ソフトウェアの SMB プロトコル プリプロセッサ検出エンジンにおける低システム メモリ サービス妨害の脆弱性により、デバイスのシステム メモリが不足し、Snort プロセスが突然再起動する可能性があります。次のエラー ログを確認した場合は Cisco Technical Assistance Center (TAC) に連絡し、デバイスで脆弱性がエクスプロイトされたかどうかを確かめることをお勧めします。

<#root>

```
Firepower-module1 kernel: [1111040.969265]
snort invoked oom-killer:
 gfp_mask=0xd0, order=0, oom_score_adj=0
```

回避策

これら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

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無償のソフトウェアアップデートをリリースしています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載のシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェ

ア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この項の該当する表に示すように、適切なリリースにアップグレードすることをお勧めします。本アドバイザリは以下のアドバイザリを含むコレクションの一部です。お客様におかれましては、これらも考慮したうえでアップグレード ソリューション全体をご確認ください。

- cisco-sa-20190501-asa-csrf:Cisco適応型セキュリティアプライアンスソフトウェアのクロスサイトリクエストフォージェリの脆弱性
- cisco-sa-20190501-asa-frpwrtd-dos:Cisco適応型セキュリティアプライアンスソフトウェアおよびCisco Firepower Threat DefenseソフトウェアのTCPタイマー処理におけるサービス妨害の脆弱性
- cisco-sa-20190501-asa-ftd-dos:Cisco適応型セキュリティアプライアンスソフトウェアおよびFirepower Threat DefenseソフトウェアのWebVPNにおけるサービス妨害の脆弱性
- cisco-sa-20190501-asa-ftd-entropy:Cisco適応型セキュリティアプライアンスソフトウェアおよびFirepower Threat Defenseソフトウェアの低エントロピーキーの脆弱性
- cisco-sa-20190501-asa-ftd-ike-dos:Cisco適応型セキュリティアプライアンスソフトウェアおよびCisco Firepower Threat DefenseソフトウェアのMOBIKEにおけるサービス妨害の脆弱性
- cisco-sa-20190501-asaftd-saml-vpn:Cisco適応型セキュリティアプライアンスソフトウェアおよびFirepower Threat DefenseソフトウェアのVPN SAML認証バイパスの脆弱性

- cisco-sa-20190501-asa-ipsec-dos:Cisco適応型セキュリティアプライアンスソフトウェアのIPsecにおけるDoS脆弱性
- cisco-sa-20190501-firepower-dos:Cisco Firepower Threat DefenseソフトウェアのTCP入力ハンドラにおけるサービス妨害の脆弱性
- cisco-sa-20190501-frpwr-dos:Cisco Firepower Threat Defenseソフトウェアのパケット処理におけるサービス妨害の脆弱性
- cisco-sa-20190501-frpwr-smb-snort:Cisco Firepower Threat DefenseソフトウェアのSMBプロトコルプリプロセッサ検出エンジンにおけるサービス妨害の脆弱性
- cisco-sa-20190501-sd-cpu-dos:Cisco適応型セキュリティアプライアンスソフトウェアおよびFirepower Threat DefenseソフトウェアのWebVPNにおけるサービス妨害の脆弱性

次の表では、左の列にシスコソフトウェアのリリースを記載しています。中央の列には、リリース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るかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。右の列は、リリースがこのアドバイザリ集に記載された何らかの脆弱性に該当するかどうか、および、それらすべての脆弱性に対する修正を含む最初のリリースを示しています。

Cisco FTD ソフトウェア

Cisco FTD ソフトウェア リリース	今回の脆弱性に対して推奨されるリリース	このアドバイザリ集で説明している脆弱性すべてに対する推奨リリース
6.0	6.2.3.12	6.2.3.12
6.0.1	6.2.3.12	6.2.3.12
6.1.0	6.2.3.12	6.2.3.12
6.2.0	6.2.3.12	6.2.3.12
6.2.1	6.2.3.12	6.2.3.12
6.2.2	6.2.3.12	6.2.3.12
6.2.3	6.2.3.12	6.2.3.12
6.3.0	脆弱性なし	6.3.0.3
6.4.0	脆弱性なし	脆弱性なし

Cisco FTD ソフトウェアの修正済みリリースにアップグレードするには、次のいずれかの操作を行います。

- Cisco Firepower Management Center（FMC）を使用して管理しているデバイスについては、FMC インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。
- Cisco Firepower Device Manager（FDM）を使用して管理しているデバイスについては、FDM インターフェイスを使用してアップグレードをインストールします。インストールが完了したら、アクセス コントロール ポリシーを再適用します。

インストールされている Snort バージョンは、FMC リリースによって異なります。

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とその公表は確認しておりません。

出典

これらの脆弱性は、Cisco TAC のサポート案件の対応時に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-frpwr-smb-snort

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	FTD ソフトウェア リリース 6.3.0.3 が使用可能になったことを示すために FTD の修正済みリリースの表を更新。	修正済みソフトウェア	Final	2019 年 5 月 2 日
1.0	初回公開リリース	—	Final	2019 年 5 月 1 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。