複数のシスコ製品におけるSnort SMB2検出エンジンのポリシーバイパスおよびDoS脆弱性

Medium

アドバイザリーID : cisco-sa-snort-smb-3nfhJtr
初公開日 : 2022-11-09 16:00
最終更新日 : 2022-11-30 21:51
バージョン 1.1 : Final
CVSSスコア : 5.8
回避策 : Yes
Cisco バグ ID : CSCwb87762 CSCwc37339 CSCwb66736 CSCwb78519 CSCvy97080 CSCwc37518 CSCwa55404 CSCwb91454

CVE-2022-20922
CVE-2022-20943

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

複数のシスコ製品でSnort検出エンジンのServer Message Block Version 2(SMB2)プロセッサに存在する複数の脆弱性により、認証されていないリモートの攻撃者が設定されたポリシーをバイパスしたり、該当デバイスでサービス妨害(DoS)状態を引き起こしたりする可能性があります。

これらの脆弱性は、Snort検出エンジンがSMB2トラフィックを処理する際のシステムリソースの不適切な管理に起因します。攻撃者は、該当デバイスを介して特定の種類のSMB2パケットを大量に送信することで、これらの脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はSnortプロセスのリロードを引き起こし、その結果DoS状態が発生する可能性があります。

注:Snort検出エンジンでsnort preserve-connectionオプションが有効になっている場合、エクスプロイトが成功すると、攻撃者が設定されたポリシーをバイパスし、保護されたネットワークに悪意のあるペイロードを配信する可能性もあります。snort preserve-connection設定は、デフォルトで有効になっています。詳細については、このアドバイザリの「詳細」セクションを参照してください。

注：この脆弱性の影響を受けるのは、Snort 3が設定されている製品だけです。Snort 2が設定されている製品は該当しません。

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。これらの脆弱性には、回避策が存在します。

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-snort-smb-3nfhJtr

このアドバイザリは、2022 年 11 月に公開された Cisco ASA、FTD、および FMC のセキュリティ アドバイザリ バンドルに含まれています。アドバイザリとリンクの一覧については、Cisco Event Response：2022 年 11 月に公開された Cisco ASA、FMC、および FTD ソフトウェア セキュリティ アドバイザリ バンドル（半期）を参照してください。

該当製品

脆弱性のある製品

公開時点で、これらの脆弱性はオープンソースのSnort 3に影響を与えました。

公開時点で脆弱性が存在していたSnort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。Snortの詳細については、Snort Webサイトを参照してください。

シスコ製品への影響

公開時点で、これらの脆弱性は、シスコソフトウェアの脆弱性のあるリリースを実行している次のシスコ製品に影響を与えました。

- Cyber Vision
- FirePOWER サービス - すべてのプラットフォーム
- Firepower Threat Defense（FTD）ソフトウェア - すべてのプラットフォーム
- Meraki MXセキュリティアプライアンス[1]
- Umbrellaセキュアインターネットゲートウェイ(SIG)

1.これらの脆弱性の影響を受けないMerakiデバイスのリストについては、このアドバイザリの「脆弱性が存在しない製品」セクションを参照してください。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

Cisco FTDソフトウェア設定の確認

Cisco FTDソフトウェアリリース7.0.0以降の新規インストールでは、Snort 3がデフォルトで実行されます。Cisco FTDソフトウェアリリース6.7.0以前を実行し、リリース7.0.0以降にアップグレードされたデバイスでは、Snort 2がデフォルトで実行されます。

FTDソフトウェアCLIを使用したCisco FTDソフトウェア設定の確認

Cisco FTDソフトウェアを実行しているデバイスでSnort 3が設定されているかどうかを確認するには、Cisco FTDソフトウェアCLIにログインし、show snort3 statusコマンドを使用します。このコマンドで次の出力が生成される場合、デバイスではSnort 3が実行されており、これらの脆弱性の影響を受けます。

```
<#root>

show snort3 status


Currently running Snort 3
```

Cisco Firepower Management Center(FMC)ソフトウェア管理デバイス用のCisco FTDソフトウェア設定の確認

Cisco Firepower Management Center(FMC)ソフトウェアによって管理されるデバイスでSnort 3が設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco FMCソフトウェアのWebインターフェイスにログインします。
2. [デバイス（Devices）] メニューから [デバイス管理（Device Management）] を選択します。
3. 適切なCisco FTDデバイスを選択します。
4. [編集（Edit）] アイコン（鉛筆の形）をクリックします。
5. Deviceタブを選択し、Inspection Engine領域を確認します。
    - Snort 2がリストされている場合、デバイスはこれらの脆弱性の影響を受けません。
    - Snort 3がリストされている場合、デバイスはこれらの脆弱性の影響を受けます。

Cisco Firepower Device Manager(FDM)ソフトウェア管理デバイスのCisco FTDソフトウェア設定の確認

Cisco Firepower Device Manager(FDM)ソフトウェアによって管理されるデバイスでSnort 3が設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco FTDソフトウェアのWebインターフェイスにログインします。
2. メインメニューから [ポリシー（Policies）] を選択します。
3. Intrusionタブを選択します。
4. [検査エンジン（Inspection Engine）] で検査エンジンのバージョンを確認します。バージョンは、Snort 2 の場合は「2」で始まり、Snort 3 の場合は「3」で始まります。
    - デバイスでSnort 2バージョンが実行されている場合、これらの脆弱性の影響を受けません。
    - デバイスでSnort 3バージョンが実行されている場合、これらの脆弱性の影響を受けます。

Cisco Defense Orchestrator管理対象デバイスのCisco FTDソフトウェア設定の確認

Cisco Defense Orchestratorによって管理されるデバイスでSnort 3が設定されているかどうかを確認するには、次の手順を実行します。

1. Cisco Defense Orchestrator Web インターフェイスにログインします。
2. Inventoryメニューから、適切なCisco FTDデバイスを選択します。
3. [デバイスの詳細（Device Details）] 領域で、[Snortバージョン（Snort Version）] を確認します。バージョンは、Snort 2 の場合は「2」で始まり、Snort 3 の場合は「3」で始まります。
    - デバイスでSnort 2バージョンが実行されている場合、これらの脆弱性の影響を受けません。
    - デバイスでSnort 3バージョンが実行されている場合、これらの脆弱性の影響を受けます。

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、これらの脆弱性が以下の製品には影響を与えないことを確認しました。

- Cisco 1000シリーズサービス統合型ルータ(ISR)
- Cisco 4000シリーズサービス統合型ルータ(ISR)
- Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Cisco Catalyst 8000V Edge ソフトウェア
- Cisco Catalyst 8200 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8300 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8500 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8500L シリーズ エッジ プラットフォーム
- Ciscoクラウドサービスルータ1000V
- Cisco Firepower Management Center（FMC）ソフトウェア
- Cisco Meraki MX64およびMX64wアプライアンス
- Cisco Meraki MX65およびMX65wアプライアンス
- シスコサービス統合型の仮想ルータ(ISRv)
- オープンソースの Snort 2

詳細

snort preserve-connectionの設定

これらの脆弱性による影響は、Snort preserve-connection設定が有効か無効か、およびSnortプロ

セスがダウンする前にトラフィックフローが開始したか、またはSnortプロセスがダウンしている間にトラフィックフローが開始したかによって、2種類あります。

Snortプロセスがダウンする前に確立されたトラフィックフローの動作は設定に依存します。Snortプロセスがダウンしている間に開始されるトラフィックフローの動作は設定に依存せず、常にDoS状態になります。snort preserve-connection設定の詳細については、『Cisco Secure Firewall Threat Defenseコマンドリファレンス』および『Firepower Management Centerコンフィギュレーションガイド』の「Snortリスタートトラフィックの動作」セクションを参照してください。

snort preserve-connectionが有効

Snort検出エンジンでsnort preserve-connectionオプションが有効になっている場合、Snortプロセスがダウンしても既存のトラフィックフローはドロップされません。代わりに、既存のトラフィックフローはSnort検出エンジンをバイパスします。エクスプロイトに成功すると、攻撃者は設定されたポリシーをバイパスし、保護されたネットワークに悪意のあるペイロードを配信できる可能性があります。Snortプロセスがダウンしている間に開始されたトラフィックフローはドロップされ、その結果DoS状態が発生します。

既存のトラフィックフローのCVSSスコアは、CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:Nです。

新しいトラフィックフローのCVSSスコアは、CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:Lです。

snort preserve-connectionが無効

Snort検出エンジンでsnort preserve-connectionオプションが無効になっている場合、既存のトラフィックフローはドロップされます。不正利用に成功すると、DoS状態が発生する可能性があります。Snortプロセスがダウンしている間に開始されたトラフィックフローもドロップされ、DoS状態が発生します。

CVSSスコアは、新しいトラフィックフローと既存のトラフィックフローの両方で同じです。CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

Cisco FTD ソフトウェア設定の確認

snort preserve-connection設定は、デフォルトで有効になっています。現在の設定を表示するには、Cisco FTDソフトウェアCLIにログインし、show running-config | include snortコマンドを使用します。設定を表示するためのGUIオプションはありません。

このコマンドで次の出力が生成される場合、デバイスでsnort preserve-connectionが有効になっています。

```
<#root>

>

show running-config | include snort


snort preserve-connection
>
```

コマンドによって次の出力が生成される場合、デバイスではsnort preserve-connectionが無効になっています。

```
<#root>

>

show running-config | include snort


no snort preserve-connection
>
```

回避策

これらの脆弱性に対処する回避策があります。Cisco FMCソフトウェアが管理するデバイスとCisco Defense Orchestratorが管理するデバイスに対するこれらの脆弱性の攻撃方法を排除するには、Snort検出エンジンをバイパスするようにfastpathプレフィルタルールを設定します。Cisco Firepower Device Manager(FDM)で管理されるデバイスに対するこれらの脆弱性の攻撃方法を排除するには、Snort検出エンジンをバイパスするようにアクセスコントロールルールを設定します。

Cisco FMCソフトウェア管理デバイスの回避策

Cisco FMCソフトウェア管理デバイスのSMBトラフィックに対してファストパスプリフィルタルールを設定するには、次の手順を実行します。

1. FMC Web インターフェイスにログインします。
2. PoliciesメニューのAccess Controlセクションで、Prefilterを選択します。
3. New Policyを選択します。
4. NameとDescriptionを入力し、Saveをクリックします。
5. 表示されたウィンドウで、Default Action: Tunnel TrafficがAnalyze all tunnel trafficに設定されていることを確認します。
6. Add Prefilter Ruleをクリックします。
7. 表示されたウィンドウで、ルールNameを入力し、Enabledボックスにチェックマークが付

いていることを確認します。
8. Actionドロップダウンメニューから、Fastpathを選択します。
9. 該当するネットワークのSMBトラフィックに対して、Interfaces、Networks、およびVlan Tagsタブでポリシーを設定します。
10. Portタブをクリックします。
11. SMBトラフィックの宛先ポートとして、TCP(6):138、TCP(6):139、TCP(6):445、UDP(17):137を入力します。
12. Addをクリックして、ポリシーを追加します。
13. Saveをクリックして、ポリシーを保存します。

SMBプリフィルタポリシーをCisco FMCソフトウェア管理デバイスに導入されたアクセスコントロールポリシーに関連付けるには、次の手順を実行します。

1. PoliciesメニューのAccess Controlセクションで、Access Controlを選択します。
2. 興味のあるポリシーを見つけます。
3. Editアイコンをクリックします。
4. Prefilter Policyの横にある名前をクリックします。
5. 新しく作成したSMBプレフィルタポリシーの名前をドロップダウンメニューから選択します。
6. [OK] をクリックします。

詳細については、『Firepower Management Center Device Configuration Guide』の「Prefiltering and Prefilter Policies」の章を参照してください。

Cisco FDM管理対象デバイスの回避策

Fastpathは、Cisco FDM管理対象デバイスではサポートされません。代わりに、適切なポートに対してtrustアクションを使用してアクセスコントロールポリシーを設定します。

Cisco FDM管理対象デバイスのSMBトラフィックをバイパスするようにアクセスコントロールポリシーを設定するには、次の手順を実行します。

1. Cisco FDM Webインターフェイスにログインします。
2. [ポリシー（Policies）] メニューから [アクセス制御（Access Control）] を選択します。
3. プラス(+)記号をクリックして、新しいポリシーを作成します。
4. 名前を入力し、ActionドロップダウンメニューでTrustを選択します。
5. Portセクションで、プラス(+)記号をクリックします。
6. Create New Portを選択します。
7. TCP(6):138、TCP(6):139、TCP(6):445、およびUDP(17):137の各ポートの名前、プロトコルタイプ、およびポート番号を入力します。
8. ポートが作成されたら、ルールに追加する4つのポートを名前で選択します。
9. 完了したら [OK] をクリックします。
10. OKをクリックしてポリシーを追加します。

11. Cisco FTDソフトウェアに対する変更を導入します。

詳細については、『Firepower Threat Defense Configuration Guide for Firepower Device Manager』の「Access Control」の章を参照してください。

Cisco Defense Orchestrator管理対象デバイスの回避策

Cisco Defense Orchestratorが管理するデバイスのSMBトラフィックに対してファストパスプリフィルタルールを設定するには、次の手順を実行します。

1. Cisco Defense Orchestrator Web インターフェイスにログインします。
2. Policiesメニューから、FTD Policiesを選択します。
3. PoliciesメニューのAccess Controlセクションで、Prefilterを選択します。
4. New Policyをクリックします。
5. NameとDescriptionを入力し、Saveをクリックします。
6. 表示されたウィンドウで、Default Action: Tunnel TrafficがAnalyze all tunnel trafficに設定されていることを確認します。
7. Add Prefilter Ruleをクリックします。
8. 表示されたウィンドウで、ルールNameを入力し、Enabledボックスにチェックマークが付いていることを確認します。
9. Actionドロップダウンメニューから、Fastpathを選択します。
10. 該当するネットワークのSMBトラフィックに対して、Interfaces、Networks、およびVlan Tagsタブでポリシーを設定します。
11. Portタブをクリックします。
12. SMBトラフィックの宛先ポートとして、TCP(6):138、TCP(6):139、TCP(6):445、およびUDP(17):137を入力します。
13. Addをクリックして、ポリシーを追加します。
14. Saveをクリックして、ポリシーを保存します。

SMBプリフィルタポリシーを、Cisco Defense Orchestratorが管理するデバイスに導入されたアクセスコントロールポリシーに関連付けるには、次の手順を実行します。

1. PoliciesメニューのAccess Controlセクションで、Access Controlを選択します。
2. 興味のあるポリシーを見つけます。
3. Editアイコンをクリックします。
4. Prefilter Policyの横にある名前をクリックします。
5. 新しく作成したSMBプレフィルタポリシーの名前をドロップダウンメニューから選択します。
6. [OK] をクリックします。

詳細については、Cisco Defense Orchestrator Webサイトを参照してください。

この回避策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および

使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

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 セキュリティ アドバイザリ 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アップグレード ソリューション一式を確認してください。

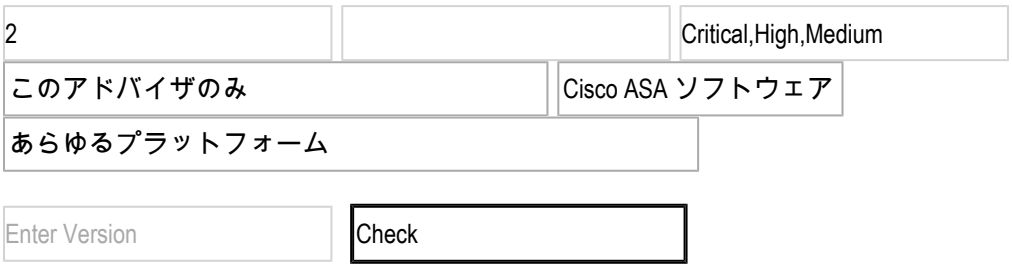
いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

Cisco ASA、FMC、およびFTDソフトウェア：CSCwb87762、CSCwb66736、CSCwa55404、CSCvy97080

お客様が Cisco ASA、FMC、および FTD ソフトウェアの脆弱性に対するリスクを判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. 検索するアドバイザリを選択します。すべてのアドバイザリ、上位および重要なアドバイザリのみ、またはこのアドバイザリのみです。
2. 該当するソフトウェアを選択します。
3. 適切なプラットフォームを選択します（Cisco ASAおよびFTDソフトウェアのみ）。
4. リリース番号を入力します。たとえば、Cisco ASA ソフトウェアの場合は 16.2.11、Cisco FTD ソフトウェアの場合は 6.6.7 と入力します。
5. [チェック（Check）] をクリックします。



FTD デバイスのアップグレード手順については、Cisco Firepower Management Center アップグレードガイドを参照してください。

サイバービジョン：CSCwc37339、CSCwc37518、CSCwb78519

発行時点では、次の表に記載されているリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

Cisco Cyber Visionリリース	CVE-2022-20922およびCVE-2022-20943の最初の修正リリース
3.x	修正済みリリースに移行。
4.0	修正済みリリースに移行。
4.1	4.1.2

Meraki MX セキュリティ アプライアンス

Cisco Meraki MXセキュリティアプライアンスリリース	CVE-2022-20922 の最初の修正済みリリース	CVE-2022-20943 の最初の修正済みリリース
MX15以前	計画なし.	修正済みリリースに移行。
MX16	計画なし.	16.16.7用のホットフィックスが利用可能
MX17	計画なし.	17.11.1用のホットフィックスが利用可能
MX18	計画なし.	18.1.3用のホットフィックス

Snort:CSCwb87762、CSCwb66736、CSCwa55404、CSCvy97080

Snortリリース	CVE-2022-20922 の最初の修正済みリリース	CVE-2022-20943 の最初の修正済みリリース
2.x	脆弱性なし	脆弱性なし
3.x	3.1.31.0	脆弱性なし

Umbrella SIG: CSCwb91454

シスコは、クラウドベースのCisco Umbrella SIGでこれらの脆弱性に対処する予定です。ユーザの対処は必要ありません。

追加情報が必要なお客様は、Cisco Umbrellaサポート(umbrella-support@cisco.com)または契約メ

ンテナンスプロバイダーにお問い合わせください。

関連情報

最適な Cisco ASA、FTD、または FMC ソフトウェアリリースの決定方法については、次の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco ASA の互換性
Cisco Secure Firewall ASA アップグレードガイド
Cisco Secure Firewall Threat Defense 互換性ガイド

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、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-snort-smb-3nfhJtr

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	Merakiホットフィックスバージョンを16.6.7から16.16.7に更新。	修正済みリリース	Final	2022年11月30日
1.0	初回公開リリース	—	Final	2022 年 11 月 9 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。

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。