Snort 2 が設定された Cisco Firepower Threat Defense ソフトウェアおよび Cisco FirePOWER サービスの ICMPv6 におけるサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-ftd-icmpv6-dos-4eMkLuN
初公開日 : 2023-11-01 16:00
最終更新日 : 2023-11-16 21:10
バージョン 1.1 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCwc20635

CVE-2023-20083

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）ソフトウェアまたは Cisco FirePOWER サービスで Snort 2 検出エンジンが設定されている場合に存在する ICMPv6 インスペクションの脆弱性により、認証されていないリモートの攻撃者が該当デバイスで CPU 使用率を 100%に引き上げてすべてのトラフィック処理を停止させ、その結果サービス妨害状態（DoS）が発生する可能性があります。FTD 管理トラフィックは、この脆弱性の影響を受けません。

この脆弱性は、ICMPv6 ヘッダー内のフィールド解析時の不適切なエラーチェックに起因します。攻撃者は、細工された ICMPv6 パケットを該当デバイスを介して送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はデバイスで CPU リソースを使い果たしてトラフィック処理を停止させ、DoS 状態を引き起こす可能性があります。

注：DoS 状態から回復するには、Snort 2 検出エンジン、Cisco FTD デバイス、Cisco FirePOWER サービスデバイスの再起動が必要になる場合があります。詳細については、このアドバイザリの「詳細情報」のセクションを参照してください。

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います。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、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-

icmpv6-dos-4eMkLuN

このアドバイザリは、2023 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：2023 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

この脆弱性は、ネットワーク検出ポリシーでホスト検出とアプリケーション検出の両方を有効にし、Snort 2 検出エンジンを呼び出すように設定されている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す。

- 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

デフォルトでは、ネットワーク検出ポリシーにはアプリケーション 検出のみが設定されています。 この脆弱性を不正利用するには、Snort 2 がアクティブである必要があります。

脆弱性が存在する Cisco 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。

ネットワーク検出ポリシー設定の確認

ネットワーク検出ポリシーでホスト検出とアプリケーション検出が設定されているかどうかを確認するには、[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] の順に選択し、[ホストおよびアプリケーション検出の基礎（Host and Application Detection Fundamentals）] を確認します。

Snort 2 ステータスの確認

Snort 2 が実行されているかどうかを確認するには、「Firepower Threat Defense（FTD）で実行されているアクティブな Snort バージョンの確認」を参照してください。

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、この脆弱性が以下のシスコ製品には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（FMC）ソフトウェア

- オープンソースの Snort 2
- オープンソースの Snort 3

詳細

この脆弱性が不正利用されると、Snort 2 検出エンジンが CPU リソースを枯渇させる可能性があります。DoS 状態から回復するには、次の 2 つの方法があります。

- Cisco FTD または Cisco FirePOWER サービスデバイスを再起動します。
- Snort 2 検出エンジンを再起動します。

Snort 2 検出エンジンの再起動

Snort 2 検出エンジンを再起動するには、次の例に示すように、エキスパートモードの CLI コマンド pmtool RestartByType de を使用します。

<#root>

```
> expert
admin@ftd:/ngfw/Volume/home/admin$

pmtool RestartByType de
```

これは中断を伴うアクションであるため、再起動する前に不正利用が発生しているかどうかを確認することを推奨します。さらに支援が必要な場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。

セキュリティ侵害の痕跡

この脆弱性が不正利用されると、CPU リソースが枯渇する可能性があります。

Snort 2 検出エンジンの CPU 使用率が高い状態にあるかの確認

Cisco FTD デバイスや Cisco FirePOWER サービスデバイスが Cisco FMC または Cisco Firepower Device Management（FDM）によって管理されている場合、管理ステーションは CPU 使用率が高いことを警告することがあります。CPU 使用率をモニタリングするには、次の例に示すように、エキスパートモードの CLI コマンド top を使用します。

<#root>

```
> expert
admin@ftd:/ngfw/Volume/home/admin$

top -p `pidof snort | sed -e "s/ /,/g"`
```

```
top - 08:03:28 up 6 days, 23:21,  2 users,  load average: 4.20, 3.19, 3.06
Tasks:   1 total,   1 running,   0 sleeping,   0 stopped,   0 zombie

%Cpu(s)

:

99.7 us

, 1.6 sy, 0.1 ni, 62.6 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem :   7899.7 total,   1483.3 free,   5743.5 used,    672.9 buff/cache
MiB Swap:   9461.2 total,   8276.2 free,   1185.0 used.   1517.3 avail Mem

PID       USER     PR   NI    VIRT         RES          SHR      S   %CPU   %MEM     TIME+       COMMAND
59156     root     1    -19   3359960      868608       35488    R

99.7

  10.7     35:08.57    snort
```

注：Cisco FTD デバイスや Cisco FirePOWER サービスデバイスでは、アクティブな Snort インスタンスが 1 つ以上存在する場合があります。

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

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。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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、お客様は以下のリンクに記載された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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

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。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情

報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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。

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。

Cisco ASA、FMC、および FTD ソフトウェア

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. ツールで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、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、またはこのアドバイザリのみを選択します。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
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 9.16.2.11、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。

2		Critical,High,Medium
このアドバイザのみ	Cisco ASA ソフトウェア	
あらゆるプラットフォーム		

Enter release number | Check

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。

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

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、シスコ内部でセキュリティ テストを実施中に、Sanmith Prakash によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-icmpv6-dos-4eMkLuN

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	Cisco FirePOWER サービスに脆弱性があることを示すために更新。	概要、脆弱性のある製品、詳細、侵害の兆候	Final	2023 年 11 月 16 日

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	2023 年 11 月 1 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。