複数のシスコ製品におけるSnort 3 MIMEのDoS脆弱性

Medium

アドバイザリーID : cisco-sa-snort3-mime-vulns-tTL8PgVH
初公開日 : 2025-10-15 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwq42153 CSCwo71401 CSCwq42161 CSCwq42141 CSCwq03467 CSCwq15864

CVE-2025-20359
CVE-2025-20360

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

HTTP Multipurpose Internet Mail Extensions(MIME)デコーダの脆弱性により、認証されていないリモートの攻撃者が、Snort 3検出エンジンで機密情報の漏洩を引き起こしたり、再起動したりすることが可能になり、複数のシスコ製品が影響を受けます。

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-snort3-mime-vulns-tTL8PgVH

該当製品

脆弱性のある製品

公開時点でこれらの脆弱性の影響を受けた製品については、次のセクションを参照してください。

オープンソースの Snort 3

公開時点で、これらの脆弱性はOpen Source Snort 3に影響を与えました。

公開時点で脆弱性が存在する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。

Cisco Secure Firewall Threat Defenseソフトウェア

公開時点で、Snort 3が設定されている場合、これらの脆弱性はCisco Secure Firewall Threat Defense(FTD)ソフトウェアに影響を与えました。

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。

Cisco Secure FTD ソフトウェアの Snort 設定の確認

Cisco Secure 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 Secure FTDソフトウェアリリース6.7.0以前を実行していて、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、デフォルトでSnort 2が実行されます。

Cisco Secure FTD ソフトウェアで Snort 3 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 バージョンの判別」を参照してください。 これらの脆弱性をエクスプロイトするには、Snort 3がアクティブである必要があります。

Cisco IOS XE ソフトウェア

公開時点で、これらの脆弱性は次のシスコ製品に影響を与えました。これらの製品では、脆弱性が存在するUnified Threat Defense(UTD)Snort IPS Engine for Cisco IOS XE SoftwareまたはUTD Engine for Cisco IOS XE SD-WAN Softwareリリースを実行している場合です。

- 1000 シリーズ サービス統合型ルータ（ISR）
- 4000 シリーズ ISR
- Catalyst 8000V エッジソフトウェア
- Catalyst 8200 シリーズ エッジ プラットフォーム
- Catalyst 8300 シリーズ エッジ プラットフォーム
- Catalyst 8500L エッジプラットフォーム
- クラウドサービスルータ 1000V
- サービス統合型仮想ルータ

注：UTDはデフォルトではこれらのデバイスにインストールされていません。UTDファイルがインストールされていない場合、デバイスはこれらの脆弱性の影響を受けません。

脆弱性のあるリリースおよび修正済みリリースの詳細については、このアドバイザリの冒頭に

記載されているバグIDを参照してください。

UTD が有効かどうかを確認する方法

デバイスでUTDが有効になっているかどうかを確認するには、show utd engine standard statusコマンドを使用します。出力のRunningの下にYesと表示されている場合、UTDは有効です。出力が表示されない場合、デバイスは影響を受けていません。次の例は、UTDが有効になっているデバイスでの出力を示しています。

<#root>

```
Router#
show utd engine standard status

Engine version       : 1.0.19_SV2.9.16.1_XE17.3
Profile              : Cloud-Low
System memory        :
             Usage  : 6.00 %
             Status : Green
Number of engines    : 1
```

<#root>

```
Engine
Running

    Health     Reason
=========================================
Engine(#1):
Yes

        Green      None
=========================================================
.
.
.
```

Cisco Meraki製品への影響

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

• MX64	• MX68	• MX100

• MX64W • MX65 • MX65W • MX67 • MX67C • MX67W	• MX68CW • MX68W • MX75 • MX84 • MX85 • MX95	• MX105 • MX250 • MX400 • MX450 • MX600

このアドバイザリの公開時点で脆弱性が存在するシスコ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。

他のシスコ製品への影響

公開時点で、これらの脆弱性はCisco Cyber Visionに影響を与えていました。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。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。

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、これらの脆弱性がオープンソースのSnort 2には影響を与えないことを確認しました。

また、シスコは、これら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。

- Cisco Secure Firewall 適応型セキュリティアプライアンス（ASA）ソフトウェア
- Cisco Secure Firewall Management Center（FMC）ソフトウェア
- Umbrellaセキュアインターネットゲートウェイ(SIG)

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2025-20359：複数のシスコ製品におけるSnort 3 MIME情報漏えいまたはDoS脆弱性

Snort 3 HTTPデコーダの脆弱性により、認証されていないリモートの攻撃者が機密データの開示を引き起こしたり、Snort 3検出エンジンをクラッシュさせたりする可能性があり、複数のシスコ製品が影響を受けます。

この脆弱性は、HTTPヘッダーのMIMEフィールドが解析される際のバッファ処理ロジックのエラーが原因です。これにより、バッファの読み取り不足が発生する可能性があります。攻撃者は、Snort 3によって解析される確立された接続を介して巧妙に細工されたHTTPパケットを送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は、Snort 3検出エンジンの予期しない再起動により、サービス拒否(DoS)状態が引き起こされる、またはSnort 3データストリームで機密情報の情報漏洩という2つの可能性のある結果のいずれかを引き起こす可能性があります。読み取り不足の状態が原因で、有効な接続データではない機密情報が返される可能性があります。

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。

バグID: CSCwq15864
CVE ID：CVE-2025-20359
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.5
CVSSベクトル： CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L

CVE-2025-20360：複数のシスコ製品でのSnort 3 MIMEに関するDoS脆弱性

Snort 3 HTTPデコーダの脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンの再起動を引き起こす可能性のある複数のシスコ製品が影響を受けます。

この脆弱性は、HTTPヘッダーのMIMEフィールドが解析される際の完全なエラーチェックの欠如に起因します。攻撃者は、確立された接続を介して巧妙に細工されたHTTPパケットを送信し、Snort 3によって解析されることで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は、Snort 3検出エンジンが予期せず再起動したときにDoS状態を引き起こす可能性があります。

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。

バグID: CSCwo71401
CVE ID：CVE-2025-20360
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

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

シスコでは、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策を検討します。これらの脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

修正済みリリース

修正済みリリースの詳細については、次の項を参照してください。

オープンソースSnortソフトウェア

発行時点では、次の表に示すリリース情報は正確でした。

Snort 3リリース	CVE-2025-20360 の最初の修正済みリリース	CVE-2025-20359 の最初の修正済みリリース
3.x	3.9.1.0	3.9.3.0

Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェア

お客様が Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェアにおける脆弱性のリスクの有無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、セキュリティへの影響の評価（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 Secure Firewall ASA ソフトウェアの場合は 9.20.3.4、Cisco Secure FTD ソフトウェアの場合は 7.4.2 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	

UTDソフトウェア用Cisco IOS XEソフトウェア

修正済みリリースの詳細については、このアドバイザリの冒頭にあるBug IDを参照してください。

Cisco Meraki

シスコでは、Cisco Merakiソフトウェアの修正を2026年2月にリリースする予定です。

Cyber Vision:CSCwq03467およびCSCwq42141

発行時点では、次の表に示すリリース情報は正確でした。

左の列にはシスコのソフトウェアリリースが、中央の列と右の列には、そのリリースがこのアドバイザリに記載された脆弱性の影響を受けるかどうかと、これらの脆弱性に対する修正を含むリリースが示されています。

Cisco Cyber Visionリリース	CVE-2025-20360 の最初の修正済みリリース	CVE-2025-20359 の最初の修正済みリリース
5.2 より前	修正済みリリースに移行。	修正済みリリースに移行。
5.2	修正済みリリースに移行。	修正済みリリースに移行。
5.3	脆弱性なし	脆弱性なし

シスコの 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済みリリース情報のみを検証します。

関連情報

最適な Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各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 Secure Firewall 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 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

CVE-2025-20360：この脆弱性は、シスコの内部セキュリティテストでArunesh Shuklaおよび Sanmith Prakashによって発見されました。

CVE-2025-20359：この脆弱性を報告していただいたTrend Micro社のTrend Research社のGuy Lederfein氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-mime-vulns-tTL8PgVH

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	2025年10月15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。