複数のシスコ製品におけるSnort 3 Visual Basic for Applicationsのサービス妨害(DoS)の脆弱性

Medium

アドバイザリーID : cisco-sa-ftd-snort3-vbavuls-96UcVVed
初公開日 : 2026-03-04 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : Yes
Cisco バグ ID : CSCwq23369 CSCwr21406 CSCwq97658 CSCwq23373 CSCwq97660 CSCwq23372 CSCwq97494 CSCwq97497 CSCwq97750 CSCwq23377 CSCwq97748

CVE-2026-20057
CVE-2026-20058
CVE-2026-20053
CVE-2026-20054

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

Snort 3 Visual Basic for Applications(VBA)の解凍エンジンでは、認証されていないリモートの攻撃者がSnort 3検出エンジンの予期しない再起動を引き起こし、その結果サービス妨害(DoS)状態が発生する可能性があるため、複数のシスコ製品が脆弱性の影響を受けます。

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-ftd-snort3-vbavuls-96UcVVed

このアドバイザリは、2026年3月に公開された『Cisco Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェアセキュリティアドバイザリバンドル』の一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: March 2026 Semiannual Cisco Secure Firewall ASA, Secure FMC, and Secure FTD Software Security Advisory Bundled Publication』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が設定されていて、少なくとも1つのSnort 3ディテクタがVBAマクロ圧縮解除用に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。

VBAマクロ圧縮解除設定の詳細は、次のとおりです。

- VBAマクロの圧縮解除は、既定では有効になっていません。
- VBA圧縮解除をサポートする最初のCisco FTDソフトウェアリリースは、リリース7.2.0です。詳細は、「バージョン7.2.0のファイアウォール管理センター機能」の表を参照してください。
- VBAマクロの圧縮解除は、IMAP、SMTP、HTTP、およびPOP3 Snort Inspectorエンジンでサポートされています。詳細については、『Snort 3インスペクタリファレンス』および『Cisco Secure Firewall Management Center Snort 3コンフィギュレーションガイド、バージョン7.2』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。 これらの脆弱性を不正利用するには、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
- 8100 シリーズ セキュアルータ
- 8200 シリーズ セキュアルータ
- 8300 シリーズ セキュアルータ
- 8400 シリーズ セキュアルータ
- 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
- Catalyst IR1800高耐久性シリーズルータ
- Catalyst IR8340高耐久性ルータ
- 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。

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。

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
=========================================================
.
.
.
```

他のシスコ製品への影響

公開時点では、脆弱性CVE-2026-20053、CVE-2026-20054、およびCVE-2026-20057がCisco Cyber Visionに該当していました。

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。

- Meraki 製品
- セキュアアクセス – セキュアインターネットアクセス(SIA)の利点
- セキュアアクセス – セキュアプライベートアクセス(SPA)の利点

- 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 Cloud-delivered Firewall(CDFW)(旧称Umbrella Secure Internet Gateway(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-2026-20053:Cisco Secure FTDソフトウェアのSnort 3 VBAヒープオーバーフローによるDoS脆弱性

Snort 3 VBA機能の脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンをクラッシュさせる可能性があり、複数のシスコ製品が影響を受けます。

この脆弱性は、ユーザ制御のVBAデータを圧縮解除する際の範囲チェックが不適切なことに起因します。攻撃者は、巧妙に細工されたVBAデータをターゲットデバイスのSnort 3検出エンジンに送信することで、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、攻撃者はヒープデータのオーバーフローを引き起こし、それが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。

Bug ID:CSCwq23373、CSCwq97494、およびCSCwq97497
CVE ID：CVE-2026-20053
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

CVE-2026-20054:Cisco Secure FTDソフトウェアのSnort 3 VBAの無限ループによるDoS脆弱性

Snort 3 VBA機能の脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンをクラッシュさせる可能性があり、複数のシスコ製品が影響を受けます。

この脆弱性は、VBAデータの圧縮解除時の不適切なエラーチェックに起因します。攻撃者は、巧妙に細工されたVBAデータをターゲットデバイスのSnort 3検出エンジンに送信することで、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検出エンジンを無限ループに陥れ、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。

Bug ID:CSCwq23372、CSCwq97748、およびCSCwq97750
CVE ID：CVE-2026-20054
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

CVE-2026-20057およびCVE-2026-20058:Cisco Secure FTDソフトウェアのSnort 3 VBAのDoS脆弱性

Snort 3 VBA機能の脆弱性により、認証されていないリモートの攻撃者がSnort 3検出エンジンをクラッシュさせる可能性があります。

これらの脆弱性は、VBAデータの圧縮解除時の不適切なエラーチェックに起因します。攻撃者は、巧妙に細工されたVBAデータをターゲットデバイスのSnort 3検出エンジンに送信することで、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 3検出エンジンを予期せず再起動させ、DoS状態を引き起こす可能性があります。

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があります。

バグID:CSCwq23369、CSCwr21406、CSCwq23377、CSCwq97658、およびCSCwq97660
CVE ID：CVE-2026-20057 および CVE-2026-20058
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があります。

このアドバイザリに記載されている脆弱性は、VBAの圧縮解除に起因するものです。この圧縮解除は、Snort 3のインスペクタではデフォルトで有効になっていません。デバイスを修正済みのソフトウェアリリースにアップグレードするまでVBAの圧縮解除を無効にしても、デバイスはこれらの脆弱性の影響を受けません。VBA設定を削除する方法の詳細については、次の参照先を参照してください。

- バージョン7.2.0のファイアウォール管理センター機能
- Snort 3インスペクタリファレンス
- Cisco Secure Firewall Management Center Snort 3コンフィギュレーションガイド、バージョン7.2

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

シスコでは、回避策や緩和策（該当する場合）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の一時的な解決策であると考えています。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-2026-20053、CVE-2026-20054、および CVE-2026-20057の最初の修正済みリリース	CVE-2026-20058 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	3.9.3.0	3.9.6.0

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	

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

UTDソフトウェア用Cisco IOS XEソフトウェア：CSCwq97494、CSCwq97748、CSCwq97658、およびCSCwr21406

発行時点では、次の表に示す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。

左の列にはシスコソフトウェアリリースが、右の列には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、および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 IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
17.12	17.12.7 （2026年3月）
17.15	17.15.5
17.18	17.18.3 (Apr 2026)
26.1	26.1.1 （2026年3月）

Cyber Vision（サイバービジョン）:CSCwq97497、CSCwq97750、および CSCwq97660

発行時点では、次の表に示す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。

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-2026-20053、CVE-2026-20054、および CVE-2026-20057の最初の修正済みリリース	CVE-2026-20058 の最初の修正済みリリース
5.3 より前	修正済みリリースに移行。	脆弱性なし
5.3	5.3.3	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。

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 Advanced Security Initiatives Group（ASIG）の Jason Crowder による内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort3-vbavuls-96UcVVed

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	2026年3月4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。