# Cisco IOS XEソフトウェア向けCisco Unified Threat Defense Snort Intrusion Prevention System Engineにおけるセキュリティポリシーバイパスおよびサービス妨害(DoS)の脆弱性

Medium

アドバイザリーID : cisco-sa-utd-snort3-dos-bypas-b4OUEwxD
CVE-2024-20508
初公開日 : 2024-09-25 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco バグ ID : CSCwj21273

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 IOS XEソフトウェア向けCisco Unified Threat Defense(UTD)Snort侵入防御システム(IPS)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設定されたセキュリティ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。

この脆弱性は、HTTP要求がCisco UTD Snort IPSエンジンによって処理される際の不十分な検証に起因します。攻撃者は、該当デバイスを介して巧妙に細工されたHTTP要求を送信することにより、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Snortプロセスのリロードを引き起こす可能性があります。 Cisco UTD Snort IPSエンジンの障害時のアクションがデフォルトのfail-openに設定されている場合、この脆弱性の不正利用に成功すると、攻撃者は設定されているセキュリティポリシーをバイパスできる可能性があります。Cisco UTD Snort IPSエンジンの障害時のアクションがfail-closeに設定されている場合、この脆弱性の不正利用に成功すると、Cisco UTD Snort IPSエンジンによって検査されるように設定されたトラフィックがドロップ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。

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-utd-

snort3-dos-bypas-b4OUEwxD

# 該当製品

## 脆弱性のある製品

公開時点では、この脆弱性は、Cisco IOS XEソフトウェア用のCisco UTD Snort IPSエンジンの脆弱性が存在するリリースを実行していて、Webフィルタリング機能またはマルチテナント機能、あるいはその両方が有効になっている次のシスコ製品に影響を与えました。

- 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 シリーズ エッジ プラットフォーム
- Catalyst IR8300 高耐久性シリーズ ルータ

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。

## デバイス設定の確認

デバイス設定を決定する方法については、次の項を参照してください。

Cisco UTD Snort IPSエンジンが有効になっているかどうかの確認

Cisco UTD Snort IPSエンジンがデバイスで有効になっているかどうかを確認するには、デバイスのCLIでshow utd engine standard statusコマンドを使用します。出力されない場合、Cisco UTD Snort IPS Engineは有効ではなく、デバイスはこの脆弱性の影響を受けません。Runningの下にYesと表示されていれば、Cisco UTD Snort IPS Engineは有効であり、デバイスが影響を受けます。次に例を示します。

<#root>

```
Router#
show utd engine standard status


Profile                 : Cloud-Low
System memory           :
             Usage  : 6.00 %
             Status : Green
Number of engines       : 1
```

```
Engine

Running

    Health     Reason
=======================================================
Engine(#1):   Yes        Green      None
=======================================================
.
.
.
```

マルチテナントが有効になっているかどうかの確認

Cisco UTD Snort IPSエンジンでマルチテナントが有効になっているかどうかを確認するには、show utd engine standard config | include Multi-tenancyコマンドをデバイスのCLIで使用します。出力がない場合、マルチテナントは無効になり、デバイスはWebフィルタリングが有効になっている場合にのみ、この脆弱性の影響を受けます。Multi-tenancyの下にEnabledと表示された場合は、Multi-Tenancyが有効になっており、Webフィルタリングの設定にかかわらず、次の例のようにデバイスが影響を受けます。

```
<#root>

Router#

show utd engine standard config | include Multi-tenancy


Multi-tenancy

: Enabled
```

Webフィルタリングが有効になっているかどうかの確認

Cisco UTD Snort IPSエンジンでWebフィルタリングが有効になっているかどうかを確認するには、show utd engine standard config | include Web-Filterコマンドをデバイスの CLIで使用します。出力にDisabledと表示される場合、または出力がない場合は、Webフィルタリングが無効になっており、マルチテナントが有効になっている場合にだけ、デバイスがこの脆弱性の影響を受けます。Web-Filterの下にEnabledと表示された場合は、Web Filteringが有効であり、次の例に示すように、マルチテナント設定に関係なくデバイスが影響を受けます。

```
<#root>

Router#

show utd engine standard config | include Web-Filter
```

```
Web-Filter
    : Enabled
```

### 設定されたフェールポリシーの確認

Cisco UTD Snort IPSエンジンの障害時に設定されたアクションを確認するには、show platform software utd global | include Fail Policyコマンドを実行することによって確認できます。次の例は、show platform software utd global | include Fail Policyコマンドを、Cisco UTD Snort IPS Engineの障害時のアクションがFail-openに設定されているデバイスで実行した場合の出力例を示します。

```
<#root>
Router#
show platform software utd global | include Fail Policy

Fail Policy
          : Fail-open
```

### 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製品には影響を与えないことを確認しました。

- 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 8500 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 Threat Defense（FTD）ソフトウェア
- シスコサービス統合型の仮想ルータ(ISRv)
- Cisco Secure Firewall Management Center(FMC)ソフトウェア（旧称：Firepower Management Center Software）
- オープンソースの Snort

## 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

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。

## 修正済みリリース

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。

左側の列にはシスコソフトウェアリリース、右側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が示されています。

| Cisco UTD Snort IPSエンジンリリース | First Fixed Release（修正された最初のリリース） |
|---|---|
| 17.12 より前 | 脆弱性なし |
| 17.12 | 17.12.4 |
| 17.13 | 修正済みリリースに移行。 |
| 17.14 | 脆弱性なし |

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やその公表は確認しておりません。

# 出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

# URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-utd-snort3-dos-bypas-b4OUEwxD

## 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 | 2024年9月25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。