Cisco Secure Firewall適応型セキュリティアプライアンスおよびSecure Firewall Threat Defenseソフトウェアロギングにおけるサービス妨害の脆弱性

Advisory ID : cisco-sa-asa-ftd-logging-dos-ZXXNesfN
CVE-2026-20154
初公開日 : 2026-09-16 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : Yes
Cisco Bug ID : CSCwq97424

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

Cisco Secure Firewall Adaptive Security Appliance(ASA)ソフトウェアおよびCisco Secure Firewall Threat Defense(FTD)ソフトウェアのsyslogメッセージ419002のシステムレート制限プロセスにおける脆弱性により、認証されていないリモートの攻撃者が該当デバイスで高いCPU使用率を引き起こし、その結果サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、syslogメッセージ419002の不適切なレート制限に起因します。攻撃者は、大量のTCP同期(SYN)パケットを該当デバイスに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。エクスプロイトに成功すると、攻撃者が高いCPU使用率を引き起こし、その結果パフォーマンスが低下す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。本脆弱性に対処する回避策がいくつかあります。

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-asa-ftd-logging-dos-ZXXNesfN

このアドバイザリは、アドバイザリグループの一部です。これらのアドバイザリとリンクの一覧については、2026年9月16日発行のCisco Advance Notification, Security Advisoriesを参照してください。また、Cisco Secure Firewall製品の改善と修正に関するさらに詳しいドキュメントについては、『Cisco Secure Firewall Adaptive Security Appliance Software、Secure Firewall Threat

Defense Software、およびSecure Firewall Management Centerソフトウェア強化リリース：2026年9月』を参照してください。

該当製品

脆弱性がある製品

この脆弱性は、Cisco Secure Firewall ASAソフトウェアまたはCisco Secure FTDソフトウェアの脆弱性が存在するリリースを実行し、メッセージ419002に対してsyslogロギングが有効になっているシスコデバイスに影響を与えます。ロギングがグローバルに有効な場合、ロギングメッセージ419002はデフォルトで有効になっています。

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。

デバイス設定の確認

デバイスがこの脆弱性の影響を受けるかどうかを確認するには、次の手順を実行します。

1. デバイスのCLIでshow logging | include syslog loggingコマンドを使用して、syslogロギングがグローバルに有効になっているかどうかを確認します。次の例に示すように、このコマンドの出力にenabledが含まれている場合は、syslogロギングはグローバルに有効になっています。ステップ 2 に進みます。

```
<#root>

ASAv1#

show logging | include syslog

Syslog logging:

enabled
```

出力にロギングが無効であると示されている場合、そのデバイスは影響を受けません。

2. show logging message 419002コマンドを使用して、syslogメッセージ419002でロギングが特に有効になっているかどうかを確認します。このコマンドの出力で、syslogメッセージ419002に対してロギングが有効になっていることが示された場合は、このメッセージをロギングするときにデバイスが使用するデフォルトレベルを記録してください。次の出力例は、syslogメッセージ419002がデフォルトレベルのwarningsで有効になっていることを示しています。ステップ 3 に進みます。

```
<#root>
```

```
ASA#
show logging message 419002

syslog 419002: default-level
warnings
 (enabled),standby
logging (disabled)
```

このメッセージのロギングが無効になっている場合、デバイスは影響を受けません。

3. show logging | include logging: level コマンドを使用して、ログの出力先へのロギングが有効になっているかどうかを確認し、対応するログレベルを確認します。
次の出力例は、ロギングが宛先コンソールのerrorsレベルと宛先バッファのwarningsレベルで有効になっていることを示しています。

```
<#root>
ASA# show logging | include logging: level

Console
 logging: level
errors
, 301 messages logged

Buffer
 logging: level
warnings
, 265964 messages logged
```

任意の宛先へのロギングが、ステップ2以降でsyslogメッセージ419002について確認されたログレベルで有効になっている場合、そのデバイスは影響を受けます。

ステップ3の例では、宛先バッファへのロギングは警告をレベル化するように設定されています。これは、ステップ2の例でsyslogメッセージ419002に対するログレベルに対応しています。この例のデバイスは、脆弱であると見なされます。

ステップ3の例では、宛先コンソールへのロギングはerrorsレベルで設定されています。これは、ステップ2の例でsyslogメッセージ419002に対してロギングされるレベルよりも低いレベルです。これがデバイスで有効になっているロギング宛先だけであれば、syslogメッセージ

419002は口グに記録されず、デバイスは脆弱であると見なされません。

show logging | include logging: level コマンドの出力が空白の場合、デバイスは影響を受けていません。

ロギング設定の詳細については、『CLI Book 1: Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide, 9.24』のロギングに関する章、Cisco Secure Firewall Management Center Device Configuration Guideの「Syslog」セクション、またはCisco Secure Firewall Device Manager Configuration Guideの「Configuring System Logging Settings」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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が Cisco Secure Firewall Management Center（FMC）ソフトウェアには影響を与えないことを確認しました。

回避策

この脆弱性に対処する回避策はありません。Cisco Secure Firewall ASAソフトウェアまたはCisco Secure FTDソフトウェアのレート制限。以下のセクションで説明する方法を使用します。

Cisco Secure Firewall ASA ソフトウェア

Cisco Secure Firewall ASAソフトウェアを実行しているデバイスの場合は、logging rate-limit 100 1 message 419002コマンドを使用して、グローバルコンフィギュレーションモードと手動でレート制限を追加します。

次の例では、メッセージ419002は1秒あたり100メッセージのレートに制限されており、この脆弱性のエクスプロイトを阻止します。

```
<#root>

ASA(config)#

logging rate-limit 100 1 message 419002
```

Cisco Secure FTDソフトウェア

Cisco Secure FTDソフトウェアを実行しているデバイスでは、次のいずれかのオプションを使用します。

- Secure Firewall Management Center (FMC) > Devices > Platform Settings > Rate Limit > Syslog Levelの順に選択し、適切なポリシーを展開します。詳細については、「FMC経由のFTDのロギングの設定」を参照してください。
- Firewall Device Manager (FTD) > Device > System Settings > Logging の順に選択すると、メッセージ419002ートが毎秒100メッセージに制限されます。詳細については、「Firepowerデバイスマネージャのsyslogの設定と確認」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

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。この脆弱性を修正し、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。

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

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

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 Cisco Cisco Technical Assistance Center（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-asa-ftd-logging-dos-ZXXNesfN

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9月16日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

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。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

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 Technical Assistance Center（TAC）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。

ソフトウェアのアップグレードを検討する際には、関連す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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、シスコ セキュリティ アドバイザリ ページをご覧ください。Cisco 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評価します。詳細については、シスコのセキュリティ脆弱性ポリシーを参照してください。

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。