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ソフトウェアのアクセスコントロールリストバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-aclbypass-dos-CVxVRSvQ
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 : No workarounds available
Cisco バグ ID : CSCwq78991

CVE-2026-20073

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 Secure Firewall適応型セキュリティアプライアンス(ASA)ソフトウェアおよびCisco Secure Firewall Threat Defense(FTD)ソフトウェアの脆弱性により、認証されていないリモートの攻撃者が、該当デバイスを経由して拒否する必要のあるトラフィックを送信できる可能性があります。

この脆弱性は、クラスタに参加している該当デバイスで、アクセス制御ルールの複製中にメモリ不足が発生した場合の不適切なエラー処理に起因します。攻撃者は、デバイスを介してブロックする必要のあるトラフィックを送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はアクセスコントロールをバイパスし、保護されたネットワーク内のデバイスに到達でき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-asaftd-aclbypass-dos-CVxVRSvQ

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

この脆弱性の公開時点では、シスコデバイスがCisco Secure Firewall ASAソフトウェアまたはSecure FTDソフトウェアの脆弱性のあるリリースを実行しており、クラスタ構成で展開されている場合に、これらのデバイスに影響が及びました。

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 Firewall ASAとセキュアFTDデバイスクラスタ設定の確認

デバイスがクラスタ展開の一部として設定されているかどうかを確認するには、デバイスのCLIで**show cluster info**コマンドを使用します。デバイスがクラスタ構成で実行されている場合、このコマンドは、次の例に示すように、クラスタ名、ステータス、クラスタノード、およびそれらの状態を含む一般的なクラスタ情報を返します。

```
# show cluster info

Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID   : 1
      Version   : 9.5(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Feb 26 2026
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID   : 1
      Version   : 9.5(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Feb 25 2026
      Last leave: N/A
  Unit "A" in state CONTROL_NODE
      ID        : 2
      Site ID   : 2
      Version   : 9.5(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Feb 25 2026
      Last leave: N/A
  Unit "B" in state DATA_NODE
      ID        : 3
```

```
Site ID   : 2
Version   : 9.5(1)
Serial No.: P3000000191
CCL IP    : 10.0.0.2
CCL MAC   : 000b.fcf8.c61e
Last join : 19:13:50 UTC Feb 25 2026
Last leave: 19:13:36 UTC Feb 25 2026
```

クラスタ設定で実行していない場合は、次の例に示すように、show cluster infoコマンドはクラスタが設定されていないことを示すか、クラスタに関連する情報を表示しません。

```
# show cluster info

Clustering is not configured
```

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。

詳細

ノードがクラスタに参加している場合、複製された構成に多数のアクセスコントロールエントリ(ACE)があるアクセスコントロールリスト(ACL)が含まれていると、ルールの複製プロセス中にメモリ不足が発生する可能性があります。 その結果、ノードが不完全なACLを持つクラスタに参加することがあり、これによって正規のトラフィックがドロップされたり、拒否されたはずのトラフィックが該当デバイスを通過できるようになる可能性があります。

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

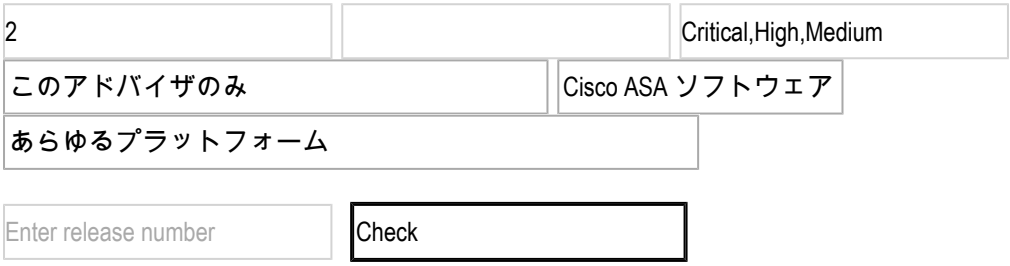
シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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。



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-asaftd-aclbypass-dos-CVxVRSvQ

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

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。