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DHCPにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-dhcp-qj7nGs4N
初公開日 : 2025-08-14 16:00
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : No workarounds available
Cisco バグ ID : CSCwm08235

CVE-2025-20135

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DHCPクライアント機能の脆弱性により、認証されていない隣接する攻撃者が使用可能なメモリを枯渇させる可能性があります。

この脆弱性は、着信DHCPパケットの不適切な検証に起因します。攻撃者は、巧妙に細工されたDHCPv4パケットを該当デバイスに繰り返し送信することで、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、攻撃者は使用可能なメモリを使い果たすことができます。これにより、サービスの可用性に影響を与え、新しいプロセスの開始が妨げられるため、サービス拒否(DoS)状態が発生し、手動によるリブートが必要になります。

注：Cisco Secure FTDソフトウェアでは、この脆弱性は管理インターフェイスには影響しません。

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-dhcp-qj7nGs4N

このアドバイザリは、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2025年8月リリースの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: August 2025 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

この脆弱性が公開された時点では、DHCPクライアント機能が有効になっており、脆弱性が存在するCisco Secure Firewall ASAソフトウェアまたはSecure FTDソフトウェアのリリースを実行しているデバイスに影響が及んでいました。

注：Cisco Secure FTDソフトウェアでは、この脆弱性の影響を受けるのはデータインターフェイスだけです。専用管理インターフェイスで受信されたDHCPトラフィックは、この脆弱性を引き起こしません。

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。

セキュアファイアウォールASAデバイスでDHCPクライアント機能が有効になっているかどうかの確認

Cisco Secure Firewall ASAソフトウェアを実行しているデバイスのインターフェイスで、DHCPクライアントが有効になっているかどうかを確認するには、show ip | include DHCPコマンドを使用して、DHCPを含む行を探します。次の例は、GigabitEthernet0/3インターフェイスでDHCPクライアントが有効になっているCisco ASAデバイスの出力を示しています。

```
firewall# show ip | include DHCP
GigabitEthernet0/3                         unassigned      unassigned      DHCP
GigabitEthernet0/3                         unassigned      unassigned      DHCP
firewall#
```

このコマンドで空の出力が返される場合、デバイスはこの脆弱性の影響を受けません。

セキュアファイアウォールASAデバイスがDHCPクライアントとして設定されているかどうかを確認する

Cisco Secure Firewall ASAソフトウェアを実行しているデバイスでDHCPクライアントが設定されているかどうかを確認するには、show running-config | include address dhcpコマンドを使用します。次の例は、インターフェイスでDHCPクライアントが設定されているCisco Secure Firewall ASAデバイスの出力を示しています。

```
ciscoasa# show running-config | include address dhcp
 ip address dhcp
ciscoasa#
```

このコマンドで空の出力が返される場合、デバイスはこの脆弱性の影響を受けません。

セキュアなFTDデバイスでDHCPクライアント機能が有効になっているかどうかの確認

Cisco Secure FTDソフトウェアを実行しているデバイスで、データインターフェイスに対してDHCPクライアントが有効になっているかどうかを確認するには、次の手順を実行します。

1. Webブラウザからデバイスの管理IPにアクセスして、Cisco Secure Firewall Device Manager(FDM)のユーザインターフェイスを開きます。
2. Interfaces > View All Interfacesの順に移動します。
3. データインターフェイスごとに、編集アイコンをクリックします。Type値がDHCPに設定されている場合、そのインターフェイスはDHCPクライアントとして設定されます。

インターフェイスが有効になっている場合、デバイスはこの脆弱性の影響を受けます。

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。

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完全なアップグレード ソリューション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。

Cisco Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェア

お客様がCisco Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェアの脆弱性による侵害の可能性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、該当する『Cisco Secure FMC upgrade guide』を参照してください。

関連情報

最適なCisco Secure Firewall ASA、Secure FMC、またはSecure FTDソフトウェアリリースの判別に関しては、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 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 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-asaftd-dhcp-qj7nGs4N

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8月14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。