Cisco適応型セキュリティアプライアンスおよびFirepower Threat Defenseソフトウェアの SNMPにおけるサービス妨害の脆弱性

アドバイザリーID : cisco-sa-asaftd-snmp-dos-7TcnzxTU
CVE-2024-20268
初公開日 : 2024-10-23 16:00
バージョン 1.0 : Final
CVSSスコア : 7.7
回避策 : No workarounds available
Cisco バグ ID : CSCwi20114 CSCwe90609

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 Firepower Threat Defense(FTD)ソフトウェアのSimple Network Management Protocol(SNMP)機能の脆弱性により、認証されたリモートの攻撃者がデバイスの予期しないリロードを引き起こす可能性があります。

この脆弱性は、SNMPパケットの不十分な入力検証に起因します。攻撃者は、IPv4またはIPv6を使用して該当デバイスに巧妙に細工されたSNMP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。エクスプロイトに成功すると、攻撃者が該当デバイスをリロードできるようになり、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、すべてのバージョンのSNMP（バージョン1、2c、および3）に影響し、有効なSNMPコミュニティストリングまたは有効なSNMPv3ユーザクレデンシャルを必要とします。

詳細については、このアドバイザリの「詳細情報」のセクションを参照してください。

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-snmp-dos-7TcnzxTU

このアドバイザリは、2024年10月に公開されたCisco ASA、FMC、および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。これらのアドバイザリとリンクの一覧については、

『シスコイベントレスポンス：Cisco ASA、FMC、およびFTDソフトウェアに関するセキュリティアドバイザリ公開半年刊2024年10月』を参照してください。

該当製品

脆弱性のある製品

リモートSNMP管理が有効になっている場合、この脆弱性はCisco ASAソフトウェアおよびCisco FTDソフトウェアに影響を与えます。

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。

SNMP設定の確認

デバイスでSNMPが有効になっているかどうかを確認するには、次のいずれかのオプションを使用します。

オプション1:Cisco ASAまたはFTDデバイス用のCLIを使用します。

show running-config snmp-server コマンドを使用します。このオプションは、Cisco ASA ソフトウェアと Cisco FTD ソフトウェアの両方で機能します。

出力に snmp-server エントリが含まれている場合、設定されている SNMP のバージョンに関係なく、システムはこの脆弱性の影響を受けます。次の例は、SNMPアクセスがSNMPv2に設定されているデバイスの出力を示しています。

```
<#root>

ASA#

show running-config snmp-server


snmp-server host
 mgmt 10.10.10.10 community snmpro version 2c
```

オプション2：管理対象のCisco FTDデバイスにCisco Secure Firewall Management Centerソフトウェアを使用します。

Cisco Secure Firewall Management Center(FMC)ソフトウェア（旧Firepower Management Center Software）によって管理されるCisco FTDデバイスに対しては、次の手順を実行します。

1. Cisco FMCソフトウェアにログインします。
2. [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] を選択します。
3. 確認するポリシーオブジェクトを選択します。
4. 左側の列でSNMPを選択します。

Enable SNMP Serversチェックボックスにチェックマークが入っていて、Hostsタブにエントリがある場合、選択したポリシーが導入されているデバイスが影響を受けます。

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 Cisco 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

SNMP は、アプリケーションレイヤ プロトコルであり、ネットワーク デバイスのモニタリングや管理で、標準化されたフレームワークおよび共通言語として使用されます。SNMP マネージャとエージェント間の通信に必要なメッセージ フォーマットを定義します。

SNMP エージェントは、デバイス パラメータおよびネットワーク データに関する情報のリポジトリである SNMP MIB からデータを収集します。また、SNMP マネージャからの要求に応答して、データの取得または設定も行います。SNMPエージェントにはMIB変数が含まれており、その値はgetまたはset操作を使用してSNMPマネージャによって要求または変更できます。

このアドバイザリで説明されている脆弱性の不正利用に使用できるのは、該当システム宛てのトラフィックに限られます。

SNMPv2c以前を使用してこの脆弱性を不正利用するには、攻撃者が該当システムのSNMP read-onlyコミュニティストリングを知っている必要があります。コミュニティ ストリングとは、デバイスの SNMP データへの読み取り専用アクセスおよび読み取り/書き込みアクセスの両方を制限するパスワードです。コミュニティ ストリングには一般的なキーワードを使用せず、他のパスワードと同様に慎重に選択してください。また、定期的にネットワーク セキュリティのポリシーに合わせて変更する必要もあります。たとえば、ネットワーク管理者がロールを変更する場合や退職する際はコミュニティ ストリングを変更する必要があります。

SNMPv3を使用してこの脆弱性を不正利用するには、攻撃者はデバイスでSNMPv3ユーザクレデンシャルを設定している必要があります。

回避策

この脆弱性に対処する回避策はありません。ただし、デバイスでSNMPが必要ない場合は、管理者はSNMPを無効にして攻撃ベクトルを阻止できます。また、信頼できるSNMPモニタリングホ

ストからのSNMP接続だけを許可することで、攻撃を受ける危険性を軽減することもできます。

この緩和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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

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。

サービス契約をご利用でないお客様

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 TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

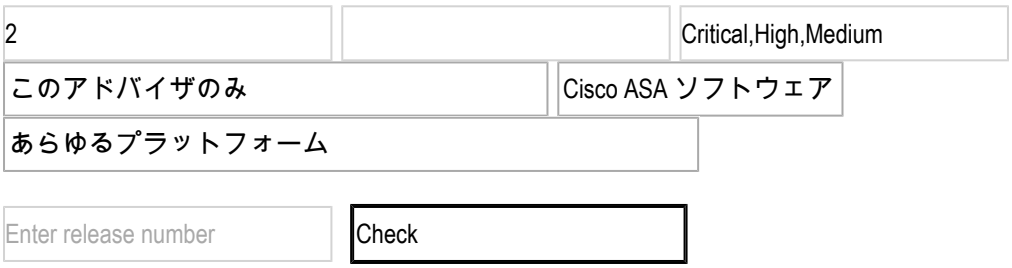
無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

Cisco ASA、FMC、および FTD ソフトウェア

お客様が Cisco ASA、FMC、および FTD ソフトウェアの脆弱性に対するリスク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、セキュリティ影響評価（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 ASA ソフトウェアの場合は 9.16.2.11、Cisco FTD ソフトウェアの場合は 6.6.7 と入力します。
5. [チェック（Check）] をクリックします。



注：Cisco ASAソフトウェアを実行しているCisco 3000シリーズ産業用セキュリティアプライアンス(ISA)については、Cisco ASAソフトウェアリリース9.16.4.67のリリースは延期されており、リリース9.16.4.70に置き換えられています。

Cisco 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 FMC upgrade guide』を参照してください。

関連情報

最適な Cisco ASA、FMC、または FTD 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 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、シスコ内部でセキュリティ テストを実施中に、Sanmith Prakash によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmp-dos-7TcnzxTU

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10月23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。