複数のシスコセキュリティ製品におけるSimple Network Management Protocolサービスの DoS脆弱性

Medium

アドバイザリーID : cisco-sa-ESA-SNMP-JLAJksWK　CVE-2022-20675
初公開日 : 2022-04-06 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCwa07400 CSCwa08629 CSCwa06167

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 Eメールセキュリティアプライアンス(ESA)、Cisco Webセキュリティアプライアンス(WSA)、およびCisco Secure Email and Web Manager（以前のセキュリティ管理アプライアンス）のTCP/IPスタック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Simple Network Management Protocol(SNMP)サービスをクラッシュさせ、サービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、TCPポート199のオープンポートリスナーに起因します。攻撃者は、TCPポート199に接続することで、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SNMPサービスをクラッシュさせ、その結果DoS状態が発生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。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-ESA-SNMP-JLAJksWK

注：シスコポートフォリオの簡素化の一環として、セキュリティ製品の名称を変更し、Cisco Secure というブランド名に統一しています。詳細については、「Cisco Secure が登場」を参照してください。

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 AsyncOSソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えました。

- ESA
- Cisco Secure Email and Web Manager
- WSA

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。

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。

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、次の表に記載されている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。

左の列はシスコソフトウェアリリースを示し、右の列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を示しています。

E メール セキュリティ アプライアンス（ESA）

Cisco AsyncOS ソフトウェアリリース	First Fixed Release（修正された最初のリリース）
13.5 以前.	脆弱性なし
14.0	14.02.0-020

Cisco Secure Email and Web Manager

Cisco AsyncOS ソフトウェアリリース	First Fixed Release（修正された最初のリリース）
12.5 以前.	修正済みリリースに移行。
13.8.1	修正済みリリースに移行。
14.0	修正済みリリースに移行。
14.1	14.1.0-239
14.2	脆弱性なし

Web セキュリティ アプライアンス（WSA）

Cisco AsyncOS ソフトウェアリリース	First Fixed Release（修正された最初のリリース）
12.0	修正済みリリースに移行。
12.5	修正済みリリースに移行。
14.0	修正済みリリースに移行。
14.5	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-ESA-SNMP-JLAJksWK

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	2022 年 4 月 6 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。