Cisco Secure Email and Web Manager、Secure Email Gateway、およびSecure Web ApplianceのSNMPポーリング情報漏えいの脆弱性

Medium

アドバイザリーID : cisco-sa-esa-sma-wsa-snmp-inf-FqPvL8sX
CVE-2025-20207
初公開日 : 2025-02-05 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 : CSCwk56456 CSCwk60819 CSCwk56452

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 Email & Web Manager、Cisco Secure Email Gateway、およびCisco Secure Web AppliancesのSimple Network Management Protocol(SNMP)ポーリングの脆弱性により、認証されたリモートの攻撃者が基盤となるオペレーティングシステムに関する機密情報を取得できる可能性があります。

この脆弱性は、アプライアンスがSNMPポーリング要求に応答して保管中の機密情報を保護しないために存在します。攻撃者は、該当アプライアンスに巧妙に細工されたSNMPポーリング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、攻撃者は、制限する必要のある機密情報を見つける可能性があります。この脆弱性をエクスプロイトするには、攻撃者がSNMPクレデンシャルを設定している必要があります。

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-sma-wsa-snmp-inf-FqPvL8sX

該当製品

脆弱性のある製品

公開時点で、次のシスコ製品でSNMPが有効にされている場合、この脆弱性の影響を受けます。

- Cisco Secure Email and Web Manager
- Secure Email Gateway
- Cisco Secure Web Appliance

注：これらの製品では、SNMPはデフォルトで有効になっていません。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。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。

SNMP が有効になっているかどうかの確認

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、SSHを使用してデバイスに接続し、snmpconfigコマンドを実行します。

次の例は、SNMPが設定されているデバイスでこのコマンドを実行した場合の出力を示しています。

```
<#root>

ESA>

snmpconfig


Current SNMP settings:
Listening on interface "Management" 10.10.10.10/27 port 161.
SNMP v3: Enabled. Security level: authPriv
Authentication Protocol: SHA
[...]
```

次に、SNMPが設定されていないデバイスでこのコマンドを実行した場合の出力例を示します。

```
<#root>

ESA>

snmpconfig
```

```
Current SNMP settings:
SNMP Disabled.
```

注：上の例は、Cisco Secure Email Gateway上でのこのコマンドの出力を示しています。該当する他の製品でのコマンドの出力は、ほぼ同じです。

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。

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。

修正済みリリース

公開時点では、次の表の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。

左側の列にはシスコソフトウェアリリース、右側の列に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が示されています。

Cisco Secure Email and Web Managerリリース	First Fixed Release（修正された最初のリリース）
15.5 以前	15.5.2-005
16.0	16.0.0-195

Cisco Secure Email Gatewayリリース	First Fixed Release（修正された最初のリリース）
15.0 以前	15.0.3-002
15.5	15.5.2-018
16.0	16.0.0-050

Cisco Secure Web Applianceリリース	First Fixed Release（修正された最初のリリース）
15.0 以前	15.0.1-004
15.1	修正済みリリースに移行。
15.2	15.2.1-010

ほとんどの場合、アプライアンスのWebベース管理インターフェイスのシステムアップグレードオプションを使用して、ネットワーク経由でソフトウェアをアップグレードできます。Webベースの管理インターフェイスを使用してデバイスをアップグレードするには、次の手順を実行します。

1. [システム管理（System Administration）] > [システムアップグレード（System Upgrade）] を選択します。
2. [アップグレード（Upgrade）] オプションをクリックします。
3. Download and Installをクリックします。
4. アップグレードするリリースを選択します。
5. [アップグレード準備（Upgrade Preparation）] 領域で、適切なオプションを選択します。
6. [続行（Proceed）] をクリックすると、アップグレードが始まります。アップグレードのステータスを示す経過表示バーが表示されます。

アップグレードが完了すると、デバイスがリブートします。

Cisco Secure Email Cloudには、サービスソリューションの一部として、Cisco Secure Email GatewayとCisco Secure Email & Web Managerデバイスが含まれています。シスコは、このソリューションに含まれる製品について、定期的なメンテナンスを行っています。お客様から Cisco TAC に連絡して、ソフトウェアのアップグレードを要求することもできます。

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-wsa-snmp-inf-FqPvL8sX

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2月5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。