Cisco IOSおよびIOS XEソフトウェアのSNMPv3設定制限の脆弱性

アドバイザリーID : cisco-sa-snmpv3-qKEYvzsy
初公開日 : 2025-05-07 16:00
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : Yes
Cisco バグ ID : CSCwk87338 CSCwi84832

CVE-2025-20151

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 IOSソフトウェアおよびCisco IOS XEソフトウェアのSimple Network Management Protocol(SNMPv3)バージョン3機能の実装における脆弱性により、デバイスが不正な送信元からのSNMPトラフィックを拒否するように設定されている場合や、設定からSNMPv3ユーザ名が削除されている場合でも、認証されたリモート攻撃者が該当デバイスにSNMPを使用してポーリングできる可能性があります。

この脆弱性は、SNMPv3設定がCisco IOSソフトウェアおよびCisco IOS XEソフトウェアのスタートアップコンフィギュレーションに保存される方法に起因します。攻撃者は、拒否されるはずの送信元アドレスから該当デバイスをポーリングすることで、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、拒否する必要のある送信元からSNMP操作を実行できる可能性があります。

注：攻撃者はSNMPv3設定を制御できません。この脆弱性を不正利用するには、攻撃者は有効なSNMPv3ユーザクレデンシャルを持っている必要があります。

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。

シスコでは、本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せん。ただし、この脆弱性の影響を受けないようにSNMPv3を設定する新しい方法があります。本脆弱性に対処する回避策がいくつかあります。

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-snmpv3-qKEYvzsy

このアドバイザリは、2025年5月に公開されたCisco IOSソフトウェアおよびIOS XEソフトウェアの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 IOSおよびIOS XEソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年5月）』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、SNMPv3機能が設定されている場合、この脆弱性はCisco IOSおよびIOS XEソフトウェアのすべてのリリースに影響を与えました。

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。

デバイス設定の確認

デバイスに影響を受ける設定があるかどうかを確認するには、このアドバイザリの「詳細」セクションのマッピングテーブルを使用します。設定行の長さが255文字を超えると、デバイスが影響を受けます。

管理者は、show snmp user usernameの出力をチェックして、access-listの名前が期待どおりに定義されているかどうかを確認することもできます。たとえば、管理者は次のようにデバイスを設定できます。

```
<#root>

Router#

configure terminal


Router(config)#snmp-server user SNMP256 SNMPV3_READ v3 auth sha auth1234567890xxxxx priv aes 256 encr
Router(config)#end
Router#

show snmp user SNMP256


User name: SNMP256
Engine ID: 80000009030074A2E6831A01
storage-type: nonvolatile        active

access-list:

 ACL-EXAMPLE-ALLOW_SNMP
Authentication Protocol: SHA
Privacy Protocol: AES256
Group-name: SNMPV3_READ

Router#
```

上記の例では、すべてが正常に見え、システムは正常に機能します。ただし、システムをリロードした場合、バックアップを開始し、同じコマンドを使用すると、管理者は次の出力を確認できます。

```
<#root>

Router#

show snmp user SNMP256


User name: SNMP256
Engine ID: 800000090300074A2E6831A01
storage-type: nonvolatile     active

access-list:

 ACL-EXAMPLE-ALLOW_S
Authentication Protocol: SHA
Privacy Protocol: AES256
Group-name: SNMPV3_READ
Router#
```

前記の例では、アクセスコントロールリスト(ACL)の名前が切り捨てられています。ACL名は設定に存在しないため、適用されず、SNMPv3ユーザにはACLが適用されません。

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、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

詳細

管理者がコンフィギュレーションCLIでSNMPv3ユーザを設定して保存すると、スタートアップコンフィギュレーションファイルに書き込まれます。認証プロトコルとプライバシープロトコルの両方の文字列は、コロンで区切られた固定長のオクテットに変換されます。キーワードのencryptedも追加されます。

これにより、次の表に示すように、保存された設定の長さが大幅に増加する可能性があります。

```
<#root>
```

Auth:

```
      MD5:    47 char to store
           SHA1:   59 char to store
           SHA256: 71 char to store
           SHA384: 95 char to store
           SHA512: 143 char to store
```

Priv:

```
      3DES:   95 char to store
           AES128: 47 char to store
           AES192: 71 char to store
           AES256: 95 char to store
```

オクテットへの変換後に設定行が255文字を超えた場合、デバイスのリロード後に実行コンフィギュレーションに読み込まれる際に、設定行が切り捨てられるか、受け入れられない場合があります。

たとえば、SNMPv3の設定は次のようになります。

```
snmp-server user SNMP256 SNMPV3_READ v3 auth sha auth1234567890xxxxx priv aes 256 encr1234567890xxxxx a
```

SNMPv3の設定は、スタートアップコンフィギュレーションで次に置き換えられます（オクテットは意図的に00のままになっています）。

<#root>

```
snmp-server user SNMP256 SNMPV3_READ v3
```

encrypted

```
 auth sha 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 priv aes 256 00:00:00:00:00:00:00
```

この例のスタートアップコンフィギュレーションは258文字で、上限の255文字を超えています。リロード時に、設定文字列の最後の3文字が削除され、ACL設定が正しくなくなります。これは、ACLが適用されていないことを意味します。

回避策

この脆弱性に対処する回避策はありません。

スタートアップコンフィギュレーションに書き込まれるSNMPv3コンフィギュレーションが255文字以下であることを確認するには、次のいずれかの方法を使用します。

- ユーザ名ではなく、SNMPv3グループ名に添付されるIPv4 ACL名、IPv6 ACL名、またはその両方を移動します。
- ユーザ名、グループ名、およびACL名の組み合わせを短くします。

この回避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

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

シスコでは、この脆弱性に対処する修正をリリースする予定はありません。

ただし、Cisco IOS XEソフトウェアリリース17.15.3および17.17.1では、Type 6暗号化を使用するSNMPv3を設定する新しい方法が導入されているため、このアドバイザリで説明されている制限を回避しながら、CLIにユーザ設定を表示できます。リリース17.15.3またはリリース17.17.1にアップグレードしても、SNMPv3設定は自動的には変換されません。管理者は、次の例に示すように、タイプ6の暗号化を使用してSNMPv3を再設定する必要があります。

```
Router#configure terminal
Router(config)#password encryption aes
Router(config)#key config-key password-encrypt Example!23
Router(config)#do show run | include snmp
Router(config)#snmp-server user test gp v3 auth sha-2 512 0 cisco1234 priv aes 128 0 cisco1234
Router(config)#do show run | include snmp
snmp-server user test gp v3 auth sha-2 512 6 GhN\ieUbTWDHFZigBYOB\eROcbV\]RLXfAAB priv aes 128 6 S`bUVJ
Router(config)#snmp-server user testUser1 PSIRTGroup v3 auth sha-2 512 0 cisco1234 priv aes 128 0 cisco
Router(config)#do sho run | include snmp
snmp-server user test gp v3 auth sha-2 512 6 GhN\ieUbTWDHFZigBYOB\eROcbV\]RLXfAAB priv aes 128 6 S`bUVJ
snmp-server user testUser1 PSIRTGroup v3 auth sha-2 512 6 RJ^DfTEg[TRTBbFHTK\fcaGPdB]ZENXFGAAB priv aes
Router(config)#
```

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 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-snmpv3-qKEYvzsy

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5月7日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。