SNMP Remote Code Execution Vulnerabilities in Cisco IOS and IOS XE Software

High

アドバイザリーID : cisco-sa-20170629-snmp
初公開日 : 2017-06-29 16:00
最終更新日 : 2025-07-30 16:27
バージョン 1.11 : Final
CVSSスコア : 8.8
回避策 : Yes
Cisco バグ ID : CSCsy56638 CSCve78027 CSCve57697 CSCve89865 CSCve60402 CSCve66658 CSCve54313 CSCve66601 CSCve60376 CSCve60276 CSCve66540

CVE-2017-6740
CVE-2017-6743
CVE-2017-6744
CVE-2017-6741
CVE-2017-6742
CVE-2017-6736
CVE-2017-6737
CVE-2017-6738
CVE-2017-6739

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 および IOS XE ソフトウェアの Simple Network Management Protocol（SNMP）サブシステムに複数の脆弱性が存在するため、認証されたリモート攻撃者により該当システムのコードがリモート実行されたり、該当システムのリロードが引き起こされたりする可能性があります。IPv4 または IPv6 経由で巧妙に細工された SNMP パケットが送信されると、脆弱性がエクスプロイトされる危険性があります。ただし本脆弱性をエクスプロイトできるのは、該当システム宛てのトラフィックに限られます。

本脆弱性は、影響を受けるソフトウェアにおける SNMP サブシステムのバッファ オーバーフロー条件に起因し、全バージョンの SNMP（バージョン 1、2c、3）に影響します。SNMP バージョン 2c 以前で本脆弱性をエクスプロイトするには、攻撃者が SNMP 読み取り専用コミュニティストリングを把握している必要があります。SNMP バージョン 3 でエクスプロイトするには、影響を受けるシステムのユーザ クレデンシャルを攻撃者が入手している必要があります。エクスプ

ロイトが成功すると、任意のコードが実行され、フル コントロールを取得されるか、影響を受けるデバイスがリロードされる危険性があります。

以下の「回避策」の項に記載されている回避策の適用をお勧めします。修正済みソフトウェアの情報は Cisco IOS Software Checker から入手できます。SNMP が有効化されており、影響を受ける MIB または OID を明示的に除外していないデバイスは、すべて脆弱であるとみなす必要があります。

シスコはこれら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。これらの脆弱性には、回避策が存在します。

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-20170629-snmp

該当製品

脆弱性のある製品

これらの脆弱性は、Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアの脆弱性が存在するリリースを実行しているシスコデバイスに影響します。これらの脆弱性は、全バージョンの SNMP (バージョン 1、2c、および 3) に影響します。

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。

脆弱性は、次のいずれかの MIB が設定されたデバイスに存在します。

- ADSL-LINE-MIB
- ALPS-MIB
- CISCO-ADSL-DMT-LINE-MIB
- CISCO-AUTH-FRAMEWORK-MIB
- CISCO-BSTUN-MIB
- CISCO-MAC-AUTH-BYPASS-MIB
- CISCO-SLB-EXT-MIB
- CISCO-VOICE-DNIS-MIB
- CISCO-VOICE-NUMBER-EXPANSION-MIB
- TN3270E-RT-MIB

SNMP が有効になっている場合には、上記の MIB はすべてデフォルトで有効になります。MIB は、すべてのシステムまたはバージョンに存在するとは限りませんが、存在する場合は有効になります。

一般的に管理者は、デバイスで有効化されている MIB のリストを表示するのに、特権 EXEC

モードの show snmp mib コマンドを使用することがあります。しかし、一部の MIB は、有効化されていても show snmp mib コマンドの出力で表示されないことがあります。ユーザには、アドバイザリの「回避策」で説明している除外リストをすべて実装することが推奨されます。

Cisco IOS ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS ソフトウェア リリースは、管理者がデバイスにログインして、CLI で show version コマンドを使用し、表示されるシステム バナーを参照することにより確認できます。デバイスが Cisco IOS ソフトウェアを実行している場合、システム バナーに「Cisco Internetwork Operating System Software」や「Cisco IOS Software」などのテキストが表示されます。バナーにはインストールされたイメージ名もカッコ内に表示され、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリース名が表示されます。一部のシスコデバイスでは、show version コマンドをサポートしていなかったり、別の出力が表示されたりします。

次の例は、Cisco IOS ソフトウェア リリースが 15.5(2)T1 で、インストールされたイメージ名が C2951-UNIVERSALK9-M であるシスコ製品を示しています。

```
<#root>

Router>

show version


Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
.
.
.
```

Cisco IOS ソフトウェアリリースの命名と番号付けの規則に関する詳細は、『White Paper: Cisco IOS and NX-OS Software Reference Guide』を参照してください。

Cisco IOS XE ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XE ソフトウェア リリースは、管理者がデバイスにログインして、CLI で show version コマンドを実行し、表示されるシステム バナーを参照することにより確認できます。デバイスが Cisco IOS XE ソフトウェアを実行している場合、システム バナーに「Cisco IOS XE Software」などのテキストが表示されます。

次に、Cisco IOS XE ソフトウェア リリース 3.16.1aS が実行されているデバイスでの show

version コマンドの出力例を示します。

```
<#root>

Router>

show version
```

```
Cisco IOS XE Software, Version 03.16.01a.S - Extended Support Release
Cisco IOS Software, ASR1000 Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.5(3)S1a, RELEASE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Nov-15 17:40 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェアリリースの命名と番号付けの規則に関する詳細は、『White Paper: Cisco IOS and NX-OS Software Reference Guide』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

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

詳細

Simple Network Management Protocol（SNMP）はアプリケーション層プロトコルであり、ネットワーク内のデバイスをモニタリングおよび管理するための標準化フレームワークおよび共通言語として機能し、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 エージェントは MIB 変数を収容します。この変数は、get または set コマンド経由で SNMP マネージャによって要求または変更されます。

これらの脆弱性は、全バージョンの SNMP（バージョン 1、2c、および 3）に影響します。影響を受けるデバイス上で、巧妙に細工された SNMP パケットを IPv4 または IPv6 経由で送信されるとエクスプロイトされる危険性があります。本脆弱性をエクスプロイトできるのは、影響を受けるデバイス宛てのトラフィックに限られます。

SNMP バージョン 2c 以前で本脆弱性をエクスプロイトするには、攻撃者が SNMP 読み取り専用コミュニティ ストリングを把握し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。

SNMP バージョン 3 でエクスプロイトするには、影響を受けるシステムのユーザ クレデンシャルを攻撃者が入手している必要があります。

セキュリティ侵害の痕跡

本脆弱性がエクスプロイトされると、該当するデバイスがリロードし、crashinfo ファイルが生成されます。Cisco Technical Assistance Center（TAC）に連絡して、このファイルを確認してもらい、これらの脆弱性を不正利用してデバイスが侵害されていないかを確認してください。

回避策

信頼できるユーザだけに SNMP アクセスを許可することが推奨されます。また、CLI で show snmp host コマンドを使用して該当システムをモニタすることも推奨されます。

さらに、デバイス上で次の MIB を無効にして脆弱性を軽減することもできます。

- ADSL-LINE-MIB
- ALPS-MIB
- CISCO-ADSL-DMT-LINE-MIB
- CISCO-AUTH-FRAMEWORK-MIB
- CISCO-BSTUN-MIB
- CISCO-MAC-AUTH-BYPASS-MIB
- CISCO-SLB-EXT-MIB
- CISCO-VOICE-DNIS-MIB
- CISCO-VOICE-NUMBER-EXPANSION-MIB
- TN3270E-RT-MIB

ビュー エントリを作成または更新して該当 MIB を無効にするには、次の例に示すように、snmp-server view グローバル コンフィギュレーション コマンドを使用できます。

```
!Standard VIEW and Security Exclusions
snmp-server view NO_BAD_SNMP iso included
snmp-server view NO_BAD_SNMP internet included
snmp-server view NO_BAD_SNMP snmpUsmMIB excluded
snmp-server view NO_BAD_SNMP snmpVacmMIB excluded
snmp-server view NO_BAD_SNMP snmpCommunityMIB excluded
snmp-server view NO_BAD_SNMP ciscoMgmt.252 excluded
!End Standard View

!Advisory Specific Mappings
!ADSL-LINE-MIB
```

```
snmp-server view NO_BAD_SNMP transmission.94 excluded

!TN3270E-RT-MIB
snmp-server view NO_BAD_SNMP mib-2.34.9 excluded

!CISCO-BSTUN-MIB
snmp-server view NO_BAD_SNMP ciscoMgmt.35 excluded

!ALPS-MIB
snmp-server view NO_BAD_SNMP ciscoMgmt.95 excluded

!CISCO-ADSL-DMT-LINE-MIB
snmp-server view NO_BAD_SNMP ciscoMgmt.130 excluded

!CISCO-AUTH-FRAMEWORK-MIB
snmp-server view NO_BAD_SNMP ciscoAuthFrameworkMIB excluded

!CISCO-VOICE-DNIS-MIB
snmp-server view NO_BAD_SNMP ciscoMgmt.219 excluded

!CISCO-SLB-EXT-MIB
snmp-server view NO_BAD_SNMP ciscoMgmt.254 excluded

!CISCO-MAC-AUTH-BYPASS-MIB
snmp-server view NO_BAD_SNMP ciscoMabMIB excluded

!CISCO-VOICE-NUMBER-EXPANSION-MIB
snmp-server view NO_BAD_SNMP ciscoExperiment.997 excluded
```

その後、コミュニティ ストリングにこのコンフィギュレーションを適用するため、次のコマンドを使用します。

```
snmp-server community mycomm view NO_BAD_SNMP RO
```

SNMP バージョン 3 の場合は次のコマンドを使用できます。

```
snmp-server group v3group auth read NO_BAD_SNMP write NO_BAD_SNMP
```

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。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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts 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。

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 Cisco Service Contract 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 POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
http://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html

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 IOS および IOS XE ソフトウェア

お客様が Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、特定のソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。 また該当する場合、そのリリースに関するすべてのアドバイザリ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。

このツールを使用して次のタスクを実行できます。

- ドロップダウン メニューからリリース（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- show version コマンドの出力をツールで解析する

- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

公開されたシスコ セキュリティ アドバイザリのいずれかに該当するリリースであるかどうかを確認するには、Cisco.com の Cisco IOS ソフトウェアチェッカーを使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアのリリース番号（たとえば、15.1(4)M2、3.1.4S など）を入力します。

Check

Cisco IOS XE ソフトウェアリリースと Cisco IOS ソフトウェアリリースのマッピングについては、Cisco IOS XE ソフトウェアリリースに応じて「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、または「Cisco IOS XE 3SG Release Notes」を参照してください。

不正利用事例と公式発表

初回公開の時点で、シスコは本アドバイザリに書かれている脆弱性の外部知識を把握しており、エクスプロイトの可能性についてお客様に通知しました。

2017 年 1 月 6 日、セキュリティ研究者がこれらの脆弱性の実用的なエクスプロイト コードを公開しました。

Cisco Product Security Incident Response Team（PSIRT）では、このアドバイザリに記載されている次の脆弱性がすでにエクスプロイトされていることを認識しています。

- CVE-2017-6736
- CVE-2017-6737
- CVE-2017-6738
- CVE-2017-6739
- CVE-2017-6740
- CVE-2017-6742
- CVE-2017-6743
- CVE-2017-6744

Cisco PSIRT は、CVE-2017-6741 で利用可能なエクスプロイトコードを把握しています。

追加情報については、『Cisco TALOS：インターネットの中核技術への信頼性を悪用する DNS ハイジャック』を参照してください。

出典

これらの脆弱性は内部テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.11	回避策に、フィルタリングに使用する MIB を追加しました。	「脆弱性のある製品」および「回避策」	Final	2025 年 7 月 30 日
1.10	これらの脆弱性が最初の修正済みリリースより前のソフトウェアにのみ影響することを明確にするために更新しました。	脆弱性が存在する製品	Final	2023 年 4 月 21 日
1.9	脆弱性のある製品を明確にするために更新。	脆弱性が存在する製品	Final	2023 年 4 月 19 日
1.8	公開されているエクスプロイトによってターゲットになる CVE を明確にするために、不正利用事例と公式発表を更新。	不正利用事例と公式発表	Final	2023 年 4 月 17 日
1.7	「エクスプロイト事例やその公表」に、確認済みの最新エクスプロイト事例を追加。	不正利用事例と公式発表	Final	2019 年 4 月 17 日
1.6	公開エクスプロイトの入手状況に関する情報を追加	不正利用事例と公式発表	Final	2018 年 1 月 11 日
1.5	Cisco Bug ID（CSCve60507）をバグリストに再び追加	Cisco Bug ID	Interim	2017 年 7 月 22 日

バージョン	説明	セクション	ステータス	日付
1.4	修正済みソフトウェアが入手可能であることを示します。Cisco IOS Software Checker へのリンクを追加しました。	修正済みソフトウェアの概要	Interim	2017 年 7 月 12 日
1.3	Added OVAL definitions.	Header	Interim	2017 年 7 月 7 日
1.2	「概要」の項に、修正済みソフトウェアと回避策に関する記述を追加しました。Cisco IOS ソフトウェア チェッカーに関する情報を削除。このツールでは問題が発生しており、矛盾したクエリの結果が表示されます。	修正済みソフトウェアの概要	Interim	2017 年 7 月 6 日
1.1	SNMP が有効になっている場合、影響を受けるバージョンおよびハードウェア構成では、影響を受けるすべての MIB がデフォルトで有効になっているという情報を「脆弱性が存在する製品」のセクションに追加。'show snmp mib' コマンドは、デバイスが影響をうけるかどうかの判断には不十分であることを「脆弱性が存在する製品」セクションに追加。脆弱な MIB と関連する除外項目を「回避策」のコンフィギュレーション コマンドに追加。	「脆弱性のある製品」、「回避策」	Interim	2017 年 7 月 3 日
1.0	初回公開リリース	—	Interim	2017 年 6 月 29 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。