

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

High	アドバイザーID : cisco-sa-20170629-snmp	<a href="#">CVE-2017-6740</a>
	初公開日 : 2017-06-29 16:00	<a href="#">CVE-2017-6743</a>
	最終更新日 : 2019-04-17 18:59	<a href="#">CVE-2017-6744</a>
	バージョン 1.7 : Final	<a href="#">CVE-2017-6741</a>
	CVSSスコア : <a href="#">8.8</a>	<a href="#">CVE-2017-6742</a>
	回避策 : Yes	<a href="#">CVE-2017-6736</a>
	Cisco バグ ID : <a href="#">CSCsy56638</a>	<a href="#">CVE-2017-6737</a>
	<a href="#">CSCve78027</a> <a href="#">CSCve57697</a>	<a href="#">CVE-2017-6738</a>
	<a href="#">CSCve89865</a> <a href="#">CSCve60402</a>	<a href="#">CVE-2017-6739</a>
	<a href="#">CSCve66658</a> <a href="#">CSCve54313</a>	
	<a href="#">CSCve66601</a> <a href="#">CSCve60376</a>	
	<a href="#">CSCve60276</a> <a href="#">CSCve66540</a>	
	<a href="#">CSCve60507</a>	

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

ドガ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、該当システム宛で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 アップデートを提供しています。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://tools.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 および IOS XE ソフトウェアの First Fixed Release より前の全リリースと、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-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。

```
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ついては、以下を参照してください。[ホワイト ペーパー：Cisco IOS および NX-OS ソフトウェア リファレンス ガイド](#)

## 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。

```
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 SOFTWARE (fcl)  
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ついては、以下を参照してください。 [ホワイトペーパー：Cisco IOS および NX-OS ソフトウェア リファレンス ガイド](#)

## 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。

本脆弱性は、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tring を把握している必要があります。コミュニティ スtring 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tring 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tring 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-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。

```
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 SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2015 by Cisco Systems, Inc.  
Compiled Wed 04-Nov-15 17:40 by mcpre  
.  
.  
.
```

その後、コミュニティ スtring 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。

```
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 SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2015 by Cisco Systems, Inc.  
Compiled Wed 04-Nov-15 17:40 by mcpre
```

SNMP バージョン 3 の場合は次のコマンドを使用できます。

```
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 SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2015 by Cisco Systems, Inc.  
Compiled Wed 04-Nov-15 17:40 by mcpre
```

## 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 アップデートを提供しています。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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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](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です。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は新規リリースでも継続して適切なサポートが受けられることを確認してください。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 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/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/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

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できるよう、シスコでは [Cisco IOS Software Checker](#) ツールを提供しています。このツールにより、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

リリースが、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かどうかを確認するには、Cisco.com の [Cisco IOS Software Checker](#) 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 リリース ( たとえば、15.1(4)M2、3.1.4S など ) を入力します。

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 ソフトウェアのリリースに応じて「[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、本アドバイザリに記載されてい

る脆弱性がすでに 익스プロイトされていることを認識しています。追加情報は次の [Cisco TALOS](#) にてご確認ください。『[DNS ハイジャック悪用 Trust In Core Internet Service](#)』

## 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://tools.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	Date
1.7	「 익스プロイト事例やその公表」に、確認済みの最新 익스プロイト事例を追加しました。	不正利用事例と公式発表	最終版	2019年4月17日
1.6	公開 익스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	最終版	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
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-July-07
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-June-29
-----	----------	--	---------	--------------

## 利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。