Cisco IOS および IOS XE ソフトウェア Layer 2 Tunneling Protocol サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20170322-l2tp

初公開日 : 2017-03-22 16:00

バージョン 1.0 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCuy82078

CVE-2017-3857

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 の機能および Cisco IOS XE ソフトウェアを解析する Layer 2 Tunneling Protocol （L2TP）の脆弱性はリモート攻撃者非認証により影響を受けたデバイスはリロードしますする可能性があります。

脆弱性は L2TP パケットの不十分な検証が原因です。 攻撃者は影響を受けたデバイスへ巧妙に細工された L2TP パケットを送信 することによってこの脆弱性を不正利用する可能性があります。正常なエクスプロイトは攻撃者により影響を受けたデバイスはサービス拒否 （DoS）状態に終って、リロードしますことを可能にする可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-l2tp

このアドバイザリは、5 脆弱性を記述する 5 Cisco Security Advisory を含む Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書のリリースの 2017 年 3月 22 日一部です。 すべての脆弱性に最高のセキュリティ への影響 定格があります。 これらのアドバイザリとリンクの一覧については、以下を参照してください。Cisco Event Response: 行進 2017 半年ごと Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書。

該当製品

脆弱性のある製品

この脆弱性は L2TP 機能がデバイスのために有効に なり、デバイスが L2TP バージョン 2（L2TPv2）または L2TP バージョン 3（L2TPv3）エンドポイントで設定されれば場合 Cisco IOS または Cisco IOS XE ソフトウェアの脆弱なリリースを実行している Ciscoデバイスに影響を与えます。 デフォルトで、L2TP 機能は有効に なりません。

脆弱性が存在する Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアのリリースについての詳細は、このアドバイザリの「修正済みソフトウェア」の項を参照してください。

L2TP 設定の査定

、管理者はデバイスにログイン L2TP がデバイスのために有効に なり、設定されるかどうか判別し、CLI を L2TPv3 pseudowire 設定または L2TP バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）設定の存在があるように確認するのに使用するためにできます。

次の例は *V3Example* と指名される pseudowire クラス設定から得られる L2TPv3 pseudowire 設定のデバイスのコンフィギュレーションの設定を示したものです:

```
pseudowire-class V3Example
 encapsulation l2tpv3
Interface GigabitEthernet0/0
 xconnect 192.0.2.3 16 encapsulation l2tpv3 pw-class V3Example
```

次の例は *例*と指名される示し、トンネリング プロトコルとして L2TP を使用したものです VPDN 設定のデバイスのコンフィギュレーションの設定を:

```
vpdn enable
vpdn-group example
 accept-dialin
  protocol l2tp
```

どちらかの設定の存在があるように確認するために、管理者は **show run を**発行できます **| VPDN を含んで下さい|pseudowire|**CLI の **xconnect** コマンドはコマンドの出力を査定したものです。 次の例は pseudowire 設定および VPDN 設定両方で L2TP を使用するために設定されるルータのコマンドの出力を示したものです:

```
Router# show run | i vpdn|pseudowire|xconnect
vpdn enable vpdn-group example pseudowire-class V3Example  xconnect 192.0.2.1 45 encapsulation
l2tpv3 pw-class V3Example
```

また、管理者は CLI でどの L2TP トンネルでもアクティブであるかどうか判別する **show vpdn コマンドを**使用できます。 次の例は 3 つのアクティブな L2TP トンネルを備えているルータのコマンドの出力を示したものです:

```
Router# show vpdn

L2TP Tunnel and Session Information Total tunnels 3 sessions 3
LocTunID    RemTunID    Remote Name    State  Remote Address  Sessn L2TP Class/
                                                              Count VPDN Group 159845550
```

```
1169197789 Router2       est    192.0.2.1         1     R2signal LocID      RemID
TunID      Username, Intf/      State  Last Chg Uniq ID                                Vcid,
Circuit 3643993064 0          159845550  16, Et0/3           wtaci  01:15:28 0 . . .
```

アクティブなトンネルが L2TP を使用していない場合、コマンド 出力は含んでいます:

```
Router# show vpdn

L2TP Tunnel and Session Information Total tunnels 3 sessions 3
LocTunID   RemTunID   Remote Name   State  Remote Address  Sessn L2TP Class/
                                                          Count VPDN Group 159845550
1169197789 Router2       est    192.0.2.1         1     R2signal LocID      RemID
TunID      Username, Intf/      State  Last Chg Uniq ID                                Vcid,
Circuit 3643993064 0          159845550  16, Et0/3           wtaci  01:15:28 0 . . .
```

このような場合、管理者はルータコンフィギュレーションを点検し、L2TP 機能が設定されないことを確認する必要があります。

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ます。その後ろには Cisco IOS ソフトウェアのリリース番号とリリース名も表示されます。 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することがあります。

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 (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
.
.
.
```

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。

シスコは、この脆弱性が Cisco IOS XR ソフトウェアまたは Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

セキュリティ侵害の痕跡

この脆弱性が不正利用されると、該当デバイスがリロードされ、crashinfo ファイルが生成されます。 不正利用はデバイスのためのスタック トレースをデコードし、*L2TP mgmt* デーモン プロセスがクラッシュしたかどうか判別することによって確認することができます。 プロセスがクラッシュしている場合は、デバイスのログか crashinfo ファイルに、次の例と同様のエラーメッセージが含まれます。

```
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
.
.
.
```

crashinfo ファイルを確認し、デバイスにこの脆弱性の不正利用が発生していないかを判別するには、Cisco Technical Assistance Center (TAC) までご連絡ください。

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

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

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

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、すべてのアドバイザリに記載されたすべて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含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全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

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のエクスプロイト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 内部テストの間に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-l2tp

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017-March-22

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。