Cisco IOS XE ソフトウェアの Locator/ID Separation Protocol における認証バイパスの脆弱性

High

アドバイザリーID : cisco-sa-20170927-lisp

初公開日 : 2017-09-27 16:00

バージョン 1.0 : Final

CVSSスコア : 8.3

回避策 : No workarounds available

Cisco バグ ID : CSCvc18008

CVE-2017-12236

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 XE ソフトウェアの Locator/ID Separation Protocol（LISP）の実装における脆弱性により、認証されていないリモート攻撃者が、X Tunnel ルータを使用し、Endpoint Identifier（EID）をマップ サーバ/マップ レゾルバ（MS/MR）の Routing Locator（RLOC）に登録する際に実行される認証チェックをバイパスする可能性があります。

この脆弱性は、影響を受けるソフトウェアのコード回帰によってもたらされた論理エラーに起因します。 攻撃者は、特定の有効なマップ登録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。この要求は、認証キーが一致しなくても MS/MR によって受け入れられます。 不正利用に成功すると、攻撃者は影響を受けるソフトウェアの MS/MR の RLOC に対して EID の無効なマッピングを行う可能性があります。

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。
927-lisp

このアドバイザリは、2017 年 9 月 27 日に公開された 13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリを含む Cisco IOS ソフトウェアおよび IOS XE ソフトウェア リリースのセキュリティ 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、以下を参照してください。シスコのイベント対応： 9月 2017 年半年ごと 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、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て、LISP が IPv4 または IPv6 マップ サーバとして動作するように設定されているシスコ デバイスに影響を及ぼします。

また、Cisco IOS XE ソフトウェア リリース トレイン 3.9E および Everest 16.4 に影響します。 Cisco IOS XE ソフトウェアがリリースする詳細については脆弱で、見ますこの状況報告の修正済みソフトウェアのセクションをであって下さい。

デバイスが LISP マップ サーバで設定されるかどうか判別するために、管理者は **show running-config を**使用できます **|** CLI にマップ **サーバ** privileged exec コマンドを**含めて下さい**。 次に、Cisco IOS XE ソフトウェアが実行され、LISP マップ サーバとして設定されているデバイスでのコマンドの出力例を示します。

```
MS/MR# show running-config | include map-server

ipv4 map-server
ipv6 map-server
MS/MR#
```

この脆弱性は、出力トンネル ルータ、入力トンネル ルータ、または単にマップ リゾルバとして LISP を実行するように設定されたデバイスには影響を及ぼしません。

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する場合、システム バナーは *Cisco IOS*ソフトウェア、*Cisco IOS XE* ソフトウェア、または同じようなテキストを表示します。

次の例は Cisco IOS XE ソフトウェア リリース 16.2.1 を実行して、*CAT3K_CAA-UNIVERSALK9-M* のインストール済みイメージ名前があるデバイスのためのコマンドの出力を示したものです:

```
ios-xe-device# show version

Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali
16.2.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 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 ソフトウェア、Cisco IOS XR ソフトウェア、および 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。

詳細

この脆弱性は、IPv4/IPv6 で不正利用される可能性があります。

セキュリティ侵害の痕跡

この脆弱性の不正利用により未知 IP アドレスは認証を行う必要があるサイトに対するマップ サーバの**提示 lisp サイト** コマンドの出力の**最後の登録されていた**カラムに現われます。

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

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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.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。
https://www.cisco.com/c/en/us/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

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

リリースがあらゆる公開された Cisco Security Advisory から影響を受けするかどうか判別するために、Cisco.com の Cisco IOSソフトウェア チェッカーを使用するか、または—次のフィールドで… Cisco IOSソフトウェアまたは Cisco IOS XE ソフトウェア リリースを—たとえば、**15.1(4)M2** か **3.13.8S** 入力して下さい:

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

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-lisp

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017 年 9 月 27 日

利用規約