Cisco IOS および NX-OS ソフトウェア Locator/ID Separation Protocol（LISP）パケット サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20160323-lisp

初公開日 : 2016-03-23 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCuv11993 CSCuu64279

CVE-2016-1351

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 Cisco Catalyst 6500 および 6800 シリーズ スイッチでおよび Cisco NX-OS ソフトウェアのの脆弱性は Locator/ID Separation Protocol（LISP）（LISP 動作する M1 シリーズ ギガビットイーサネットモジュールによって Cisco Nexus 7000 および Nexus 7700 シリーズでスイッチ動作する）リモート攻撃者非認証により脆弱 な デバイスのリロードを引き起こすようにする可能性があります。

脆弱性は不正 な LISP パケットヘッダーが受け取られるとき適切な入力の検証の欠如が原因です。 攻撃者は UDP ポート 4341 の不正 な LISP パケットの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者によりサービス拒否（DoS）状態を引き起こ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。

このアドバイザリは、次のリンクより確認できます。

323-lisp

このアドバイザリは、6 脆弱性を記述する 6 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 2016 年 3月 23 日一部です。 すべての脆弱性にあります「最高のセキュリティ へ の 影響 定格が」。 それらへの

アドバイザリおよびリンクの完全なリストに関しては、 Cisco イベント応答が表示されて下さい : 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

Cisco Catalyst 6500 はおよび Cisco NX-OS ソフトウェアを実行する M1 シリーズ ギガビット イーサネットモジュールによって Cisco IOSソフトウェアが、および Cisco Nexus 7000 および Nexus 7700 シリーズ スイッチは稼働している 6800 シリーズ スイッチ LISP が設定されるとき脆弱です。 LISP はどちらかのプラットフォームでデフォルトで有効に なりません。

情報に関してはどのについての Cisco IOS および NX-OS ソフトウェア バージョンが脆弱であるか、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下さい。

Cisco Catalyst 6500 および 6800 シリーズ スイッチ

LISP サポートはリリース 15.1(1)SY1 で最初に導入されました。 LISP がデバイスで設定されたかどうか確認するために、 **show running-config を**使用して下さい **|** 、 **ルータ lisp が**設定される次の例に示すようにかどうか見るために **lisp** コマンドを **含んで下さい**:

```
iosRouter# show running-config | include lisp
router lisp
```

Cisco IOS ソフトウェア リリースの判別

、管理者はデバイスにログインどの Cisco IOS ソフトウェア リリースが Cisco製品で動作しているか判別し、システムバナーを表示する **show version コマンドを**発行するためにできます。 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。 カッコ内にイメージ名が表示され、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続きます。

次の例は c6880x-ADVENTERPRISEK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 15.2(1)SY1 を実行している Cisco製品を指定したものです:

```
iosRouter# show version
Cisco IOS Software, c6880x Software (c6880x-ADVENTERPRISEK9-M), Version 15.2(1)SY1, RELEASE
SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 11-May-15 00:26 by prod_rel_team
.
.
.
```

Cisco IOS ソフトウェア リリースの命名規則については、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]

Nexus 7000 および 7700 シリーズ スイッチ

Nexus 7000 および 7700 シリーズ スイッチはソフトウェア リリース 5.2(1)の LISP サポートを追加しました。 LISP が設定されている Nexus 7000 および 7700 シリーズ スイッチは LISP パケットが M1 シリーズ ギガビットイーサネットモジュールで入力されるときだけ脆弱です。 **show module を**使用して下さい | 、M1 モジュールが Nexus 7000 シャーシにインストールされている次の例に示すようにかどうかチェックするために **M1** コマンドを **含んで下さい**:

```
nxosRouter# show module | include M1
3    48     10/100/1000 Mbps Ethernet XL Module N7K-M148GT-11L     powered-up
```

インストールされる M1 シリーズ ギガビットイーサネットモジュールがある場合 LISP パケットがこのモジュールで設定されるインターフェイスに入力されるときだけ脆弱です。 LISP 機能が有効に なるかどうかチェックするために、 **提示機能を**使用して下さい **| lisp** コマンドを、次次の例 **含んで下さい**:

```
nxosRouter# show feature | include lisp
lisp                  1         enabled
```

提示 IP lisp コマンドが M1 インターフェイスのための LISP 設定を決定するのに使用することができます:

```
nxosRouter# show ip lisp
LISP IP Configuration Information for VRF "default" (iid 1)
  Ingress Tunnel Router (ITR):enabled
  Egress Tunnel Router (ETR):disabled
  Proxy-ITR Router (PTR):disabled
  Proxy-ETR Router (PETR):disabled
  Map Resolver (MR):disabled
  Map Server (MS):disabled
  LISP Multicast:disabled
.
.
.
```

Nexus 7000 および 7700 シリーズ スイッチ LISP 設定に関する詳細については、 [Locator/ID Separation Protocol (LISP) 設定を]参照して下さい。

Cisco NX-OS ソフトウェア リリースを判別して下さい

Cisco NX-OS ソフトウェアを、管理者は Cisco Nexus 7000 シリーズで切り替える動作しているデバイスにログインできます判別し、 **show version コマンドを**発行することはリリースします。 次の例は 6.2(14) リリースを識別したものです:

```
nxosRouter# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2015, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
Software
  BIOS:      version 2.12.0
  kickstart: version 6.2(14)
  system:    version 6.2(14)


.
.
.
```

注: 次の Cisco M1 シリーズ ギガビットイーサネットモジュール シリーズモジュールは Cisco NX-OS リリース 7.3(0)D1(1) 現在でもはやサポートされません:

- N7K-M148GT-11
- N7K-M132XP-12
- N7K-M148GS-11

詳細については、 Cisco Nexus 7000 シリーズ NX-OS リリース ノートの **サポートされていないハードウェア** セクションを 、リリース 7.3 参照して下さい。

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。

Cisco はこの脆弱性が Cisco IOS XR および Cisco IOS XE に影響を与えないことを確認しました。

Cisco 7600 シリーズ ルータこの脆弱性から影響を受けません。

詳細

LISP ネットワークアーキテクチャおよびプロトコルは 2 新しい名前空間の作成によって IP アドレッシングのための新しい意味を設定します: エンドポイントID （ EID ）、エンドホストに割り当てられる、およびグローバル な ルーティング システムを構成するデバイス (主に ルータ) に割り当てられるルーティング ロケーター (RLOCs) 。 分割 EID および RLOC 機能はルーティング システム スケーラビリティ、マルチホーミング効率および入トラフィック エンジニアリングを改善します。 LISP 端サイト サポートは Ciscoルータのようなデバイスで設定されます。 この脆弱性は LISP パケットが影響を受けたインターフェイスで入力される LISP 設定のあらゆる型のため

にあります。

M1 シリーズ ギガビットイーサネットモジュールが付いている Cisco Catalyst 6500 および 6800 シリーズ スイッチおよび Cisco Nexus 7000 および 7700 シリーズ スイッチは不正 な LISP パケットが受信されるときクラッシュする可能性があるよくある ASIC を共有します。 不正利用されるべきこの脆弱性に関しては LISP パケットは LISP のためのよく知られたポート番号である UDP ポート番号 4341 に、UDP LISP ヘッダ 不正である必要があります向かいヘッダ 長は不正確である必要があります。

Cisco で Catalyst 6500 および 6800 シリーズはデバイスの完全なリロードという結果にこの脆弱性を終ります切り替えます。 インストールされる M1 シリーズ ギガビットイーサネットモジュールが付いている Cisco Nexus 7000 および 7700 シリーズ スイッチで M1 モジュール自体はリロードしますが、シャーシの残りは安定 して いる残ります。

セキュリティ侵害の痕跡

on Cisco Catalyst 6500 によりおよび 6800 シリーズ スイッチは、この脆弱性のエクスプロイトデバイスは **EARL 回復パッチ エラー**のリセット理由とリロードします。

on Cisco Nexus 7000 および 7700 シリーズは M1 シリーズ ギガビットイーサネットモジュールによって、この脆弱性 **致命的な割り込み首都 Device エラー**のリセット理由とリロードするために引き起こします M1 モジュールを切り替えます。

Cisco Technical Assistance Center（TAC）はデバイスがこの脆弱性から影響を受けたかどうか確認するためにシステムログ ログ· ファイルを検討する必要があります。

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。
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場合は、http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、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 Technical Assistance Center（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 ソフトウェア

顧客が Cisco IOSソフトウェアの脆弱性への公開を判別するのを助けるために Cisco はツールを、各アドバイザリに説明がある脆弱性を解決する以前のリリースおよび特定の Cisco IOS ソフトウェア リリースに影響を与える Cisco Security Advisory を識別する Cisco IOSソフトウェア チェッカー提供します、（「最初に」固定される）。 該当する場合、ツールはまた以前のリリースを戻します識別されるすべてのアドバイザリに説明があるすべての脆弱性を解決する（「結合される最初に」固定される）。

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 リリースを—たとえば、**15.1(4)M2** 入力して下さい:

Cisco NX-OS ソフトウェア

この脆弱性はソフトウェア バージョン 7.3(0)D1(1) で解決されます。 Cisco Nexus 7000 および Nexus 7700 シリーズ ソフトウェアは Cisco.com の Software Center からアクセス http://www.cisco.com/cisco/software/navigator.html および **ダウンロード ホーム > 製品 > スイッチ > データセンター スイッチ > Nexus 7000 シリーズ スイッチを**選択することによってダウンロードすることができます。

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 TAC によって処理された顧客 の 例の解決の間に発見されました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-lisp

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2016-March-23

利用規約