多重シスコ製品 OSPF LSA 操作脆弱性

Medium	**アドバイザリーID :** cisco-sa-20170727-ospf **初公開日 :** 2017-07-27 16:00 **最終更新日 :** 2017-08-03 14:07 **バージョン 2.0 :** Final **CVSSスコア :** 4.2 **回避策 :** Yes **Cisco バグ ID :** CSCva74756 CSCve47401 CSCvf28683 CSCve47393	CVE-2017-6770

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

複数のシスコ製品は Open Shortest Path First（OSPF）ルーティング プロトコル リンク状態アドバタイズメント（LSA）データベースを含む脆弱性から影響を受けます。 この脆弱性は非認証、リモート攻撃者が OSPF 自律 システム（AS）ドメイン ルーティング テーブルの完全な制御を引き継ぐことを可能にする可能性がありま代行受信するように攻撃者かブラックホール トラフィックがします。

攻撃者は細工 された OSPF パケットのインジェクトによってこの脆弱性を不正利用する可能性があります。 不正利用の成功により目標とされたルータはルーティング テーブルをフラッシュし、OSPF AS ドメイン全体の巧妙に細工された OSPF LSA タイプ 1 アップデートを伝搬させます可能性があります。

この脆弱性を不正利用するために、攻撃者は正確にターゲットルータの LSA データベース内のある特定のパラメータを判別する必要があります。 この脆弱性は巧妙に細工された ユニキャストまたはマルチキャスト OSPF LSA タイプ 1 パケットの送信によってしか引き起こすことができません。 他の LSA 型パケットはこの脆弱性を引き起こすことができません。

ファブリック 最短パス第 1（FSPF）プロトコルはこの脆弱性から影響を受けません。

この脆弱性に対処する回避策は利用できます。

このアドバイザリは、次のリンクより確認できます。

727-ospf

該当製品

脆弱性のある製品

この脆弱性は OSPF 実装の以下のシスコ製品に影響を及ぼします。 修正済みソフトウェアの情報に関しては修正済みソフトウェアのセクションを参照して下さい。

注: この脆弱性は OSPF マルチキャスト アドレスを目標とするか、または直接 OSPF使用可能な インターフェイスを目標とすることによってだけことができます引き起こす。

FSPF はこの脆弱性から影響を受けません。

Cisco IOS および Cisco IOS XE ソフトウェア

Cisco IOS か Cisco IOS XE ソフトウェアを実行しているおよび OSPF のために設定されて脆弱です Ciscoデバイスは。 有効に なる OSPF がないデバイスはこの脆弱性から影響を受けません。

OSPFv3 はこの脆弱性から影響を受けません。

Cisco IOS または Cisco IOS XE デバイスがインターフェイスの OSPF を使う場合設定されたかどうか確認するために、 **show ip ospf interface コマンドを**使用して下さい。 次の例は OSPF で設定され、GigabitEthernet0/0/1 インターフェイスで有効に なる Cisco IOSデバイスの **show ip ospf interface コマンド**の出力です:

```
Router# show ip ospf interface
GigabitEthernet0/0/1 is up, line protocol is up Internet Address 192.168.2.4/24, Area 0,
Attached via Network Statement Process ID 1, Router ID 10.10.10.4, Network Type BROADCAST,
Cost: 1 Topology-MTID    Cost    Disabled    Shutdown      Topology Name       0
1         no          no            Base Transmit Delay is 1 sec, State DR, Priority 1 . . .
```

Cisco製品で動作している Cisco IOS XE ソフトウェア、管理者 デバイスにログイン し、システムバナーを表示する **show version コマンドを**発行できますリリースして下さいか Cisco IOS を判別するために。 システムバナーはデバイスが *Cisco Internetwork Operating System software* か *Cisco IOSソフトウェアこと*をと同じようなテキストを表示するによって Cisco IOSソフトウェアを実行していることを確認します。 括弧内のイメージ名 ディスプレイ、 バージョンおよび Cisco IOS ソフトウェアリリース名によって続かれて。 他のシスコ デバイスでは、 **show version** コマンドが存在しなかったり、別の出力が表示されたりします。

次の例は *C3900-UNIVERSALK9-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 15.0(1)M1 を実行している Cisco製品を指定したものです:

```
Router# show version
```

```
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 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]

Cisco Adaptive Security Appliance

Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェアを実行している OSPF のために設定されて脆弱であり、Ciscoデバイスは。 有効に なる OSPF がないデバイスはこの脆弱性から影響を受けません。

OSPFv3 はこの脆弱性から影響を受けません。

Cisco ASA デバイスがインターフェイスの OSPF を使う場合設定されたかどうか確認するために、 **提示 OSPFインターフェイス要約**コマンドを使用して下さい。 次の例は OSPF で設定され、内部インターフェイスで有効に なる Cisco ASA デバイスの **提示 OSPFインターフェイス要約**コマンドの出力です:

```
ciscoasa# show ospf interface brief
Interface    PID   Area    IP Address/Mask         Cost  State Nbrs F/C
inside       1     1       10.10.10.1/255.255.255.0  10    WAIT 0/0
ciscoasa#
```

Cisco ASA、Cisco ASA-SM、または Cisco PIX セキュリティ アプライアンス モデルで動作しているソフトウェアのバージョンを判別するために、CLI からの **show version コマンドを**使用して下さい。 以下は **show version コマンド**からの出力の例です:

```
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.3(1)
ciscoasa#
```

Cisco NX-OS ソフトウェア

Cisco NX-OS ソフトウェアを実行している OSPF のために設定されて脆弱であり、Ciscoデバイスは。 有効に なる OSPF がないデバイスはこの脆弱性から影響を受けません。 Cisco NX-OS デバイスがインターフェイスの OSPF を使う場合設定されたかどうか確認するために、提供される例と同じような Cisco IOS および Cisco IOS XE ソフトウェア セクションで **show ip ospf interface コマンドを**使用して下さい。

Nexus 3000 を on Cisco 実行している Cisco NX-OS ソフトウェアのバージョンを判別するために、5000 は、6000、7000 および 9000 シリーズ デバイス、CLI からの **show version コマンドを**使用します。 以下は **show version コマンド**からの出力の例です:

```
switch# show version | grep system:
  system:    version 7.3(1)D1(1)
switch#
```

Cisco Nexus デバイスの脆弱性を不正利用することは Cisco Nexus デバイスのローカルルーティングプロトコルに影響を与えません。 ただし、Cisco Nexus デバイスは OSPF領域のその他のデバイスに巧妙に細工された LSA をインストールし、伝搬させます。 同じ OSPF AS の一部である他のルータに伝搬する巧妙に細工された LSA は OSPF AS を渡るルーティング テーブルに影響を与えるかもしれません。

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、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Cisco IOS XR ソフトウェア
- Cisco StarOS ソフトウェア
- Cisco Connected Grid ルータ
- Cisco Nexus 1000v シリーズ

詳細

OSPF は RFC 2328 によって定義されるルーティング プロトコルです。 AS の中の IP ルーティングを管理することを設計します。 OSPF パケット使用 IP プロトコル第 89。

OSPFプロトコルを作動させる影響を受けたネットワークデバイスはこの脆弱性によって巧妙に細工された LSA タイプ 1 パケットを受信する場合影響を与えられるかもしれません。 このパケットは確認される必要がないしスプーフィングされた IP アドレスから起きることができます。

この脆弱性を不正利用するために、攻撃者は OSPF Designated Router （ DR ）のターゲットルータ、LSA DB シーケンス番号および Router ID のネットワーク 配置および IP アドレスのようないくつかのファクタを、判別する必要があります。 攻撃者はこの脆弱性を不正利用するためにファクタすべてを知る必要があります。

OSPF プロセス ユニキャスト パケット、またマルチキャスト パケットが、この脆弱性リモートで不正利用し、ローカルセグメントの複数のシステムを同時に目標とするのに使用することができるので。 回避策に記述されているように OSPF認証を使用するセクションはこの脆弱性の効果を軽減できます。 OSPF認証を使用する強く推奨されたセキュリティ上の推奨事項はこの脆弱性の存在に関係なく、あります。

処理されて、巧妙に細工された LSA タイプ 1 パケットにより目標とされたルータはルーティングテーブルのコンテンツをフラッシュし、OSPF領域全体の巧妙に細工された LSA アップデートを伝搬させますかもしれません。 同じエリアの OSPF メンバー ルータは対象ルータによって伝搬した巧妙に細工された LSA タイプ 1 パケットを処理し、インストールすることから影響を受けま

す。 これはブラック ホールに送信 される OSPFルーティング テーブル、攻撃者によって制御される宛先にリダイレクトされるトラフィックまたはトラフィックにインジェクトされる偽ルーティングのようないくつかの結果の、原因となるかもしれません。

影響を受けたシステムを回復 するために、管理者は影響を受けたデバイスから OSPF 設定を削除し、それを再度有効に することができます。 また、リロードが影響を受けたシステムを回復 するために必要となります。 **クリア IP OSPFプロセス**または clear ip route のようなコマンドによって OSPFプロセスかルーティング テーブルをクリアすることは効果をもたらさないし、影響を受けたシステムを回復 するのに使用することができません。

セキュリティ侵害の痕跡

この脆弱性の不正利用により目標とされたルータは ID 情報が **show ip ospf database コマンド**の製品同等の出力のアドバタイズ ルータ ID を一致する ルータリンク状態 LSA データベースの矛盾した情報があります。 この脆弱性はルータISA だけ (LSA タイプ 1) 影響を与えます。

以下はこの脆弱性から影響を受ける Cisco IOS、Cisco IOS XE および Cisco NX-OS デバイスの **show ip ospf database コマンド**の出力です:

```
Router# show ip ospf database
    OSPF Router with ID (10.10.10.1) (Process ID 1)
    Router Link States (Area 0)
    Link ID         ADV Router      Age    Seq#  Checksum Link count
    10.10.10.4      10.10.10.4      334    0x8000000E 0x00E29A 3
    10.10.10.1      192.168.27.11   22     0x80000011 0x0062A8 3
    10.10.10.2      10.10.10.2      298    0x80000018 0x00394A 2
    10.10.10.3      10.10.10.3      305    0x80000020 0x00E715 3
```

以下はこの脆弱性から影響を受ける Cisco ASA デバイスの **提示 OSPFデータベースコマンド**の出力です:

```
ciscoasa# show ospf database



OSPF Router with ID (192.168.1.2) (Process ID 1)
Router Link States (Area 0)
Link ID         ADV Router      Age    Seq#  Checksum Link count
10.10.10.4      10.10.10.4      334    0x8000000E 0x00E29A 3
10.10.10.1      192.168.27.11   22     0x80000011 0x0062A8 3
10.10.10.2      10.10.10.2      298    0x80000018 0x00394A 2
10.10.10.3      10.10.10.3      305    0x80000020 0x00E715 3 . . .
```

注: 影響を受けた目標とされたルータは OSPF領域全体の巧妙に細工された LSA を伝搬させます。 脆弱性が正常に不正利用される場合、同じ OSPF領域のルータ全員は OSPF LSA データベースの巧妙に細工された LSA タイプ 1 エントリのコピーを備えています。

回避策

本脆弱性に対処する回避策がいくつかあります。 OSPF認証の使用は最良の方法と軽減として使用する必要があります。 有効なキーのない OSPF パケットは処理されません。 MD5認証は強く推奨されています、プレーンテキスト 認証の固有弱さが原因で。 非暗号化テキスト認証によって、認証鍵はローカルネットワーク セグメントの攻撃者がパケットのスニッフィングによってキーをキャプチャ することを可能にすることができるネットワークに非暗号化送信 されます。

OSPF認証に関する詳細については http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtml を参照して下さい。

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

顧客が Cisco IOS および IOS XE 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、各アドバイザリに解決する以前のリリースおよび特定のソフトウェア 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）説明がある脆弱性を。 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、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。

Cisco ASA、Cisco FTD、および Cisco NX-OS ソフトウェア

修正済みソフトウェア リリースの詳細については、本アドバイザリ上部の Cisco Bug ID を参照ください。

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

この脆弱性は発見され、ラファエルからの先生による Gabi Nakibly Cisco に報告されて防衛 システムを進めました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170727-ospf

改訂履歴

Version	Description	Section	Status	日付
2.0	Nexus 9000 デバイス、Nexus 3000 OSPFv3 で設定されるデバイスおよび NX-OS ソフトウェアが含まれる更新済脆弱なプロダクト 情報。	該当製品	Final	2017-August-03
1.1	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	Final	2017-July-28
1.0	初回公開リリース		Final	2017-July-27

利用規約