複数のシスコ製品におけるOSPF LSA操作の脆弱性

Medium

アドバイザリーID : cisco-sa-20170727-ospf CVE-2017-6770
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

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

Open Shortest Path First(OSPF)ルーティングプロトコルのリンクステートアドバタイズメント(LSA)データベースに関連する脆弱性が、複数のシスコ製品に影響を与えています。この脆弱性により、認証されていないリモートの攻撃者がOSPF自律システム(AS)ドメインのルーティングテーブルを完全に制御できるようになり、攻撃者がトラフィックを代行受信またはブラックホール化できる可能性があります。

攻撃者は、巧妙に細工されたOSPFパケットを挿入することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、ターゲットルータがルーティングテーブルをフラッシュし、OSPF ASドメイン全体に細工されたOSPF LSAタイプ1アップデートを伝播する可能性があります。

この脆弱性を不正利用するには、攻撃者はターゲットルータのLSAデータベース内の特定のパラメータを正確に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パケットを送信することによってのみ引き起こされます。他のLSAタイプのパケットでは、この脆弱性を引き起こすことはできません。

Fabric Shortest Path First(FSPF)プロトコルは、この脆弱性の影響を受けません。

この脆弱性に対処する回避策があります。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170727-ospf

該当製品

脆弱性のある製品

この脆弱性は、OSPFを実装する次のシスコ製品に影響を与えます。修正済みソフトウェアについては、「修正済みソフトウェア」のセクションを参照してください。

注：この脆弱性は、OSPFマルチキャストアドレスをターゲットにするか、OSPF対応インターフェイスを直接ターゲットにすることでのみ引き起こすことができます。

FSPFはこの脆弱性の影響を受けません。

Cisco IOSおよびCisco IOS XEソフトウェア

Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアを実行し、OSPFが設定されているシスコデバイスには脆弱性が存在します。OSPFが有効になっていないデバイスは、この脆弱性の影響を受けません。

OSPFv3は、この脆弱性の影響を受けません。

Cisco IOSまたはCisco IOS XEデバイスでインターフェイスのOSPFが設定されているかどうかを確認するには、 show ip ospf interfaceコマンドを使用します。OSPFが設定されていて、GigabitEthernet0/0/1インターフェイスで有効になっているCisco IOSデバイスでの show ip ospf interfaceコマンドの出力例を次に示します。

<#root>

```
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
.
.
.
```

シスコ製品上で実行されているCisco IOSまたは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、 show versionコマンドを発行することにより確認できます。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ることで、デバイスでCisco IOSソフトウェアが稼働していることを確認できます。カッコ内にイメージ名が表示され、その後に バージョンとCisco IOSソフトウェアリリース名が続きます。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、シスコ製品でCisco IOSソフトウェアリリースが15.0(1)M1で、インストールされたイメージ名が C3900-UNIVERSALK9-Mであることを示しています。
<#root>

```
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ソフトウェアのリリース命名規則の追加情報は、『 White Paper: Cisco IOS and NX-OS Software Reference Guide』で確認できます。

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、OSPFが設定されているシスコデバイスには脆弱性が存在します。OSPFが有効になっていないデバイスは、この脆弱性の影響を受けません。

OSPFv3は、この脆弱性の影響を受けません。

Cisco ASAデバイスが、インターフェイスでOSPFを使用して設定されているかどうかを確認するには、 show ospf interface briefコマンドを使用します。次の例は、OSPFが設定されていて、内部インターフェイスが有効になっているCisco ASAデバイスでの show ospf interface briefコマンドの出力です。

<#root>

```
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で実行されている

ソフトウェアのバージョンを確認するには、CLIで show versionコマンドを使用します。 show versionコマンドの出力例は次のとおりです。

```
<#root>

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、OSPFが設定されているシスコデバイスには脆弱性が存在します。OSPFが有効になっていないデバイスは、この脆弱性の影響を受けません。Cisco NX-OSデバイスでインターフェイスのospfが設定されているかどうかを確認するには、「Cisco IOSおよびCisco IOS XEソフトウェア」セクションの例に類似した show ip ospf interfaceコマンドを使用します。

Cisco Nexus 3000、5000、6000、7000、および9000シリーズデバイスで実行されている Cisco NX-OSソフトウェアのバージョンを確認するには、CLIで show versionコマンドを使用します。 show versionコマンドの出力例は次のとおりです。

```
<#root>

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しても、Cisco Nexusデバイスのローカルルーティングテーブルには影響しません。ただし、Cisco Nexusデバイスは、細工されたLSAをインストールし、OSPFエリア内の他のデバイスに伝播します。同じOSPF ASの一部である他のルータに伝達された巧妙に細工されたLSAが、OSPF AS全体のルーティングテーブルに影響する可能性があります。

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で定義されているルーティングプロトコルです。AS内のIPルーティングを管理するように設計されている。OSPFパケットはIPプロトコル番号89を使用します。

OSPFプロトコルを実行する該当ネットワークデバイスは、巧妙に細工されたLSAタイプ1パケットを受信すると、この脆弱性の影響を受ける可能性があります。このパケットは確認応答される必要はなく、スプーフィングされたIPアドレスから発信できます。

攻撃者がこの脆弱性を不正利用するには、ターゲットルータのネットワーク配置とIPアドレス、LSA DBシーケンス番号、OSPF代表ルータ(DR)のルータIDなど、さまざまな要因を判別する必要があります。攻撃者がこの脆弱性を不正利用するには、すべての要因を知っている必要があります。

OSPFはマルチキャストパケットだけでなくユニキャストパケットも処理するため、この脆弱性はリモートから不正利用される可能性があり、ローカルセグメント上の複数のシステムを同時に標的にするために使用される可能性があります。「回避策」セクションで説明されているOSPF認証を使用すると、この脆弱性の影響を緩和できます。OSPF認証の使用は、この脆弱性の存在にかかわらず、セキュリティのベストプラクティスとして強く推奨されます。

一度処理されると、巧妙に細工されたLSAタイプ1パケットにより、ターゲットルータがルーティングテーブルの内容をフラッシュし、巧妙に細工されたLSAアップデートをOSPFエリア全体に伝播する可能性があります。同じエリアのOSPFメンバーのルータは、標的ルータによって伝搬される巧妙に細工されたLSAタイプ1パケットを処理してインストールすることで影響を受けます。これにより、OSPFルーティングテーブルに挿入された偽のルート、ブラックホールに送信されたトラフィック、または攻撃者によって制御される宛先にリダイレクトされたトラフィックなど、さまざまな結果が発生する可能性があります。

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、再度有効にすることができます。あるいは、該当するシステムを回復するためにリロードが必要です。 clear ip ospf processや clear ip routeなどのコマンドを使用してOSPFプロセスまたはルーティングテーブルをクリアしても効果はなく、該当するシステムの回復にこのコマンドを使用することはできません。

セキュリティ侵害の痕跡

この脆弱性が工クスプロイトされると、ターゲットルータのルータリンクステートLSAデータベ

ースに矛盾した情報が保持される原因になります。この場合、リンクID情報は、 show ip ospf databaseコマンドの相当する製品の出力に含まれるアドバタイジングルータIDと一致しません。この脆弱性は、ルータLSA（LSAタイプ1）のみに影響します。

この脆弱性の影響を受けるCisco IOS、Cisco IOS XE、Cisco NX-OSデバイスで実行した show ip ospf databaseコマンドの出力を次に示します。

```
<#root>

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
```

この脆弱性の影響を受けるCisco ASAデバイスで実行した show ospf databaseコマンドの出力を次に示します。

```
<#root>

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：該当するターゲットルータは、OSPFエリア全体に細工されたLSAを伝播します。この脆弱性の不正利用に成功すると、同じOSPFエリア内のすべてのルータで、OSPF LSAデータベースに細工されたLSAタイプ1エントリのコピーが作成されます。

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、ベストプラクティスとして、また緩和策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。プレーンテキスト認証には本質的な弱点があるため、MD5認証を強く推奨します。プレーンテキスト認証では、認証キーは暗号化されずにネットワーク経由で送信され、ローカルネット

ワークセグメントの攻撃者がパケットをスニッフィングしてキーを取得できる可能性があります。

OSPF認証についての詳細は、http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtmlを参照してください。

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リリースしています。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、アクセスまたはその他の方法で使用した場合、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、[シスコのセキュリティアドバイザリおよびアラート（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(http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html)に連絡してアップグレードを入手してください。

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

お客様が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を受ける可能性を判断できるように、シスコでは Cisco IOS Software Checkerツールを提供しています。このツールによって、特定のソフトウェアリリースに影響を与えるシスコセキュリティアドバイザリと、各アドバイザリで説明されている脆弱性を修正する最初のリリース（初回修正）を特定できます。必要に応じて、このツールは、特定されたすべてのアドバイザリに記載されているすべての脆弱性を修正する最初のリリース（総合初回修正）も返します。

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。

オン

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。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

出典

この脆弱性は、Rafael Advanced Defense SystemsのGabi Nakibly博士によって発見され、シスコに報告されました。

URL

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

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.0	脆弱性のある製品情報を更新し、Nexus 9000デバイス、Nexus 3000デバイス、およびOSPFv3が設定されたNX-OSソフトウェアを含めました。	該当製品	Final	2017年8月3日
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年7月28日
1.0	初回公開リリース	—	Final	2017年7月27日

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。