複数のシスコ製品の OSPF LSA 操作脆弱性

Medium	**アドバイザリーID :** cisco-sa-20130801-lsaospf **初公開日 :** 2013-08-01 16:00 **最終更新日 :** 2017-02-13 14:29 **バージョン 1.4 :** Final **CVSSスコア :** 5.8 **回避策 :** Yes **Cisco バグ ID :** CSCug34485 , CSCug63304 , CSCug39762 , CSCug39795 , CSCug34469	CVE-2013-0149

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、ブラックホール トラフィックおよび代行受信する トラフィックの完全 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引き起こす可能性があります。 不正利用の成功により目標とされたルータのルーティング テーブルのフラッシュ、または OSPF AS ドメイン全体の巧妙に細工された OSPF LSA タイプ 1 アップデートの伝搬を引き起こ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 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。

OSPFv3 はこの脆弱性から影響を受けません。 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。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130801-lsaospf

該当製品

修正済みソフトウェア

以下のシスコ製品に OSPF 実装がありますこの脆弱性から影響を受ける。 修正済みソフトウェアの情報に関してはソフトウェア バージョン および 修正 セクションを参照して下さい。

Cisco IOS ソフトウェア

Cisco IOS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。

注: この脆弱性は有効に なる OSPF である直接ターゲット インターフェイスか OSPF マルチキャスト アドレスを目標とすることによってしか引き起こすことができません。

OSPFv3 はこの脆弱性から影響を受けません。 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。

Cisco IOS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。 以下は 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
<output truncated>
```

この脆弱性はルータISA （ LSA タイプ 1 だけ ）に影響を与えます。 この脆弱性の不正利用の結果、目標とされたルータに ID 情報が **show ip ospf database コマンド**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。
以下はこの脆弱性から影響を受ける Cisco IOS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
<output truncated>
```

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。

Cisco製品で動作している Cisco IOS ソフトウェア リリースを判別するために、管理者は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。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他の Cisco 機器では、 show version コマンドがない場合や、表示が異なる場合があります。

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 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
<output truncated>
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide" で確認できます:

http://www.cisco.com/web/about/security/intelligence/ios-ref.html

注: Cisco IOS XR はこの脆弱性から影響を受けません。

Cisco IOS XE ソフトウェア

Cisco IOS XE 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デバイスで動作している Cisco IOS XE ソフトウェアのバージョンは Command Line Interface （ CLI ）からの **show version コマンド**を使用して判別することができます。

Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA）、Cisco ASA サービスモジュール（ASA-SM）および Cisco PIX Firewall

Cisco ASA か Cisco PIX Software 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。

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は CLI からの **show version コマンド**を使用して判別することができます。

Cisco Firewall Services Module（FWSM）

Cisco FWSM 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 FWSM で動作しているソフトウェアのバージョンは CLI からの **show version コマンド**を使用して判別することができます。

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。

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は CLI からの **show version コマンド**を使用して、5000、6000 および 7000 シリーズ デバイス判別することができます。

Cisco Nexus デバイスの脆弱性を不正利用することは Cisco Nexus 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そのような巧妙に細工された 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。

注: Cisco Nexus 1000v シリーズはこの脆弱性から影響を受けません。

Cisco ASR 5000

Cisco StarOS 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 ASR 5000 で動作しているソフトウェアのバージョンは CLI からの **show version コマンド**を使用して判別することができます。

脆弱性を含んでいないことが確認された製品

以下のシスコ製品はこの脆弱性から影響を受けません:

- Cisco IOS XR ソフトウェア
- Cisco Connected Grid ルータ
- Cisco Nexus 1000v シリーズ
- Cisco Nexus 9000 シリーズ
- Cisco 次世代 ワイヤリング クローゼット（NGWC）

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。

改訂履歴

Version	Description	Section	Status	日付
1.4	脆弱性から影響を受けない製品のリストへの Cisco 追加された Nexus 9000。	該当製品-脆弱性が存在しない製品	Final	2017-February-13
1.3	含まれた NX-OS ソフトウェア 表			2014-July-31
1.2	含まれた楕円形定義			2013-August-17
1.1	固定壊れたリンク			2013-August-05
1.0	初版リリース			2013-August-01

利用規約

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。