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-20130801-lsaospf
CVE-2013-0149
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

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

複数のシスコ製品が、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の影響を受けます。この脆弱性により、認証されていない攻撃者がOSPF自律システム(AS)ドメインルーティングテーブル、トラフィックのブラックホール化、およびトラフィックのインターセプトを完全に制御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、この脆弱性を引き起こす可能性があります。不正利用に成功すると、対象ルータのルーティングテーブルがフラッシュされ、OSPF ASドメイン全体に細工されたOSPF LSAタイプ1アップデートが伝播され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決定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パケットを送信することによってのみ引き起こされます。その他の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。

OSPFv3は、この脆弱性の影響を受けません。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-20130801-lsaospf

該当製品

脆弱性のある製品

次のシスコ製品には、この脆弱性の影響を受けるOSPFが実装されています。 修正済みソフトウェアについては、「ソフトウェアバージョンと修正」セクションを参照してください。

Cisco IOS ソフトウェア

Cisco IOSソフトウェアが稼働し、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。

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が有効なインターフェイスを直接ターゲットにすることによってのみ引き起こされます。

OSPFv3は、この脆弱性の影響を受けません。 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。

Cisco IOS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 ip ospf interfaceコマンドを使用します。OSPFが設定され、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コマンドの出力を次に示します。

```
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>
```

この脆弱性の影響を受けるのは、ルータLSA（LSAタイプ1）のみです。 この脆弱性のエクスプロイトの結果、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ます。この場合、リンクID情報は、 show ip ospf databaseコマンドの出力に表示されるアドバタイジングルータIDと一致しません。
次に、この脆弱性の影響を受けるCisco IOSデバイスでの show ip ospf databaseコマンドの出力を示します。

<#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
<output truncated>
```

注：該当するターゲットルータは、OSPFエリア全体に巧妙に細工された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データベース内の巧妙に細工されたLSAタイプ1エントリのコピーが保持されます。

シスコ製品で実行されているCisco IOS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。"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、シスコ製品がCisco IOSソフトウェアリリース15.0(1)M1を実行し、インストールされているイメージ名がC3900-UNIVERSALK9-Mであることを示しています。

```
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
<output truncated>
```

Cisco IOSソフトウェアのリリース命名規則の追加情報は、次のリンクの「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、この脆弱性の影響を受けません。

Cisco IOS XE ソフトウェア

Cisco IOS XEソフトウェアを実行し、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。

シスコデバイスで実行されているCisco IOS XEソフトウェアのバージョンを確認するには、コマンドラインインターフェイス(CLI)で show versionコマンドを使用します。

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

Cisco ASAまたはCisco PIX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 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は、CLIから show versionコマンドを使用して確認できます。

Cisco Firewall Services Module（FWSM）

Cisco FWSM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 FWSM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から show versionコマンドを使用します。

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 Nexus 3000、5000、6000、および7000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は、CLIから show versionコマンドを使用して確認できます。

Cisco Nexusデバイスの脆弱性を不正利用しても、Cisco Nexus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、OSPFエリア内の他のデバイスに対して、巧妙に細工されたLSAをインストールして伝搬します。このような巧妙に細工されたLSAが同じOSPF ASに属する他のルータに伝搬されると、OSPF AS全体のルーティングテーブルに影響を与える可能性があります。

注：Cisco Nexus 1000vシリーズは、この脆弱性の影響を受けません。

Cisco ASR 5000

Cisco StarOS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 ASR 5000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から show versionコマンドを使用します。

脆弱性を含んでいないことが確認された製品

次のシスコ製品は、この脆弱性の影響を受けません。

- 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
- シスコの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。

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。

複数のシスコ製品が、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の影響を受けます。この脆弱性により、認証されていない攻撃者がOSPF自律システム(AS)ドメインルーティングテーブル、トラフィックのブラックホール化、およびトラフィックのインターセプトを完全に制御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、この脆弱性を引き起こす可能性があります。不正利用に成功すると、対象ルータのルーティングテーブルがフラッシュされ、OSPF ASドメイン全体に細工されたOSPF LSAタイプ1アップデートが伝播され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決定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パケットを送信することによってのみ引き起こされます。その他の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。

OSPFv3は、この脆弱性の影響を受けません。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。

OSPFプロトコルを実行している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アドレスから発信される可能性があります。
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はユニキャストパケットとマルチキャストパケットを処理するため、この脆弱性はリモートから悪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対象と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。

OSPFの設定の詳細については、
http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/iro_cfg.html#wp1054174を参照してください。

いったん処理されると、直接対象のルータは、巧妙に細工されたLSAタイプ1パケットによってルーティングテーブルの内容をフラッシュされ、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メンバルータは、犠牲ルータによって伝播された巧妙に細工されたLSAタイプ1パケットの処理とインストールの影響を受けます。 これにより、OSPFルーティングテーブルへの偽ルートの注入、トラフィックのブラックホール化、攻撃者によって制御される宛先へのトラフィックのリダイレクトなど、さまざまな結果が生じ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。または、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は使用できません。

注：Cisco IOSソフトウェア、Cisco IOS XEソフトウェア、Cisco ASAソフトウェア、Cisco PIXソフトウェア、およびCisco FWSMソフトウェアのすべての未修正バージョンが、この脆弱性の影響を受けます。該当するソフトウェアを実行しているターゲットデバイスは、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パケットをOSPFエリア全体に伝搬します。

この脆弱性は、次のCisco Bug IDに記述されています。

- Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアのCSCug34485(登録ユーザ専用)。Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2013-0149が割り当てられています。
- Cisco ASAおよびCisco Pix用のCSCug34469(登録ユーザ専用)。Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2013-0149が割り当てられています。
- Cisco FWSMのCSCug39762(登録ユーザ専用)にCommon Vulnerabilities and Exposures(CVE)IDとしてCVE-2013-0149が割り当てられています。
- Cisco NX-OSソフトウェアのCSCug63304(登録ユーザ専用)にCommon Vulnerabilities and Exposures(CVE)IDとしてCVE-2013-0149が割り当てられています。
- Cisco StarOSソフトウェアのCSCug39795(登録ユーザ専用)にCommon Vulnerabilities and Exposures(CVE)IDとしてCVE-2013-0149が割り当てられています。

回避策

OSPF認証の使用は有効な回避策です。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固有の弱点があるため、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るため、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キャプチャす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。

また、部分的な回避策として、OSPFの存続可能時間(TTL)セキュリティチェックを適用できます。
注：この回避策は、リモートでトリガーされる攻撃から保護するために有効であり、脆弱なデバ

イスにレイヤ2で隣接する攻撃者からは保護されません。

Interior Gateway Protocol(IGP)全般の強化の詳細については、http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtmlを参照してください。

ネットワーク内のCiscoデバイスに適用可能な他の対応策は、このアドバイザリに関連するCisco適用対応策速報を次のリンク先で参照できます。
https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=29974

修正済みソフトウェア

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。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。

Cisco IOS ソフトウェア

次のCisco IOSソフトウェアテーブルの各行は、Cisco IOSソフトウェアトレインに対応しています。特定のトレインに脆弱性が存在する場合、修正を含む最も古いリリースが「最初の修正済みリリース」列に表示されます。2013年3月のFirst Fixed Release for All Advisories Bundled Publication列には、Cisco IOSソフトウェアセキュリティアドバイザリバンドル公開で公開されたすべての脆弱性を修正する最初のリリースが記載されています。可能な場合は、利用可能な最新のリリースにアップグレードすることをお勧めします。

Cisco IOS Software Checkerを使用すると、特定のCisco IOSソフトウェアリリースに対応するシスコセキュリティアドバイザリを検索できます。このツールは、Cisco Security(SIO)ポータル(https://sec.cloudapps.cisco.com/security/center/selectIOSVersion.x)で利用できます。

メジャー リリース	修正済みリリースの入手可能性
Affected 12.0-Based Releases	First Fixed Release（修正された最初のリリース）
12.0S	12.0(1)Sまでのリリースには脆弱性はありません。
12.0SY	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。

12.0SZ	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
Affected 12.2-Based Releases	First Fixed Release（修正された最初のリリース）
12.2BX	脆弱性あり。最初の修正はリリース12.2SB
12.2DA	脆弱性あり。最初の修正はリリース15.1M
12.2EWA	脆弱性あり。最初の修正はリリース12.2SG
12.2EX	脆弱性あり。最初の修正はリリース15.0SE
12.2EY	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2EZ	12.2(60)EZ
12.2IRA	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRB	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRC	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRF	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRG	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IRH	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IRI	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IXF	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IXG	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2IXH	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2MC	脆弱性あり。最初の修正はリリース15.1M
12.2MRA	脆弱性あり。最初の修正はリリース12.2SRE
12.2MRB	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2S	脆弱性あり。最初の修正はリリース12.2SB
12.2SB	12.2(33)SB15
12.2SCA	脆弱性あり。最初の修正はリリース12.2SCG
12.2SCB	脆弱性あり。最初の修正はリリース12.2SCG
12.2SCC	脆弱性あり。最初の修正はリリース12.2SCG

12.2SCD	脆弱性あり。最初の修正はリリース12.2SCG
12.2SCE	脆弱性あり。最初の修正はリリース12.2SCG
12.2SCF	脆弱性あり。最初の修正はリリース12.2SCG
12.2SCG	12.2(33)SCG5
12.2SCH	脆弱性なし
12.2SE	12.2(55)SE8
12.2SEG	12.2(25)SEG4より前のリリースには脆弱性があり、12.2(25)SEG4以降のリリースには脆弱性はありません。最初の修正はリリース15.0SE
12.2SG	12.2(53)SG10
12.2SGA	脆弱性あり。最初の修正はリリース12.2SG
12.2SM	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SQ	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SRA	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRB	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRC	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRE	12.2(33)SRE9
12.2STE	脆弱性なし
12.2SV	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SVD	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SVE	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2SW	脆弱性あり。最初の修正はリリース15.1M
12.2SXF	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。「IOS Software Modularity Patch」を参照してください。
12.2SXH	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。「IOS Software Modularity Patch」を参照してください。
12.2SXI	12.2(33)SXI12
12.2日本語	12.2(33)SXJ6
12.2SY	脆弱性あり。最初の修正はリリース15.0SY
12.2WO	脆弱性あり。最初の修正はリリース15.0SG
12.2XNA	Cisco IOS XE ソフトウェアの可用性を参照してください。

12.2XNB	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XNC	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XND	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XNE	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XNF	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XO	脆弱性あり。最初の修正はリリース12.2SG
12.2YT	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.2ZYA	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
Affected 12.3-Based Releases	First Fixed Release（修正された最初のリリース）
12.3B	脆弱性あり。最初の修正はリリース15.1M
12.3BC	脆弱性あり。最初の修正はリリース12.2SCG
12.3BW	脆弱性あり。最初の修正はリリース15.1M
12.3JA	12.3(4)JA2より前のリリースには脆弱性があり、12.3(4)JA2以降のリリースには脆弱性はありません。12.4JAの任意のリリースに移行
12.3JEA	脆弱性なし
12.3JEB	脆弱性なし
12.3JEC	脆弱性なし
12.3JED	脆弱性なし
12.3JEE	脆弱性なし
12.3JK	12.3(2)JK3 までのリリースには脆弱性はありません。 12.3(8)JK1以降のリリースには脆弱性はありません。最初の修正はリリース15.1M
12.3JL	脆弱性なし
12.3JX	脆弱性なし
12.3T	脆弱性あり。最初の修正はリリース15.1M
12.3TPC	12.3(4)TPC11a までのリリースには脆弱性はありません。
12.3XA	12.3(2)XA7より前のリリースには脆弱性があり、12.3(2)XA7以降のリリースには脆弱性はありません。最初の修正はリリース15.1M
12.3XB	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.3XC	脆弱性あり。最初の修正はリリース15.1M
12.3XD	脆弱性あり。最初の修正はリリース15.1M
12.3XE	脆弱性あり。最初の修正はリリース15.1M
12.3XF	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得

	」セクションの手順に従って、サポート組織にお問い合わせください。
12.3XG	脆弱性あり。最初の修正はリリース15.1M
12.3XI	脆弱性あり。最初の修正はリリース12.2SB
12.3XJ	脆弱性あり。最初の修正はリリース15.1M
12.3XK	脆弱性あり。最初の修正はリリース15.1M
12.3XL	脆弱性あり。最初の修正はリリース15.1M
12.3XQ	脆弱性あり。最初の修正はリリース15.1M
12.3XR	脆弱性あり。最初の修正はリリース15.1M
12.3XU	脆弱性あり。最初の修正はリリース15.1M
12.3XW	脆弱性あり。最初の修正はリリース15.1M
12.3XX	脆弱性あり。最初の修正はリリース15.1M
12.3XY	脆弱性なし
12.3XZ	脆弱性あり。最初の修正はリリース15.1M
12.3YD	脆弱性あり。最初の修正はリリース15.1M
12.3YF	脆弱性あり。最初の修正はリリース15.1M
12.3YG	脆弱性あり。最初の修正はリリース15.1M
12.3YI	脆弱性あり。最初の修正はリリース15.1M
12.3YJ	脆弱性あり。最初の修正はリリース15.1M
12.3YK	脆弱性あり。最初の修正はリリース15.1M
12.3YM	脆弱性あり。最初の修正はリリース15.1M
12.3YQ	脆弱性あり。最初の修正はリリース15.1M
12.3YS	脆弱性あり。最初の修正はリリース15.1M
12.3YT	脆弱性あり。最初の修正はリリース15.1M
12.3YU	脆弱性あり。最初の修正はリリース15.1M
12.3YX	脆弱性あり。最初の修正はリリース15.1M
12.3YZ	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.3ZA	脆弱性あり。最初の修正はリリース15.1M
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）
12.4	脆弱性あり。最初の修正はリリース15.1M
12.4GC	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4JA	脆弱性なし
12.4JAL	脆弱性なし
12.4ジャム	脆弱性なし
12.4JAN	脆弱性なし

12.4JAX	脆弱性なし
12.4JAZ	脆弱性なし
12.4JDA	脆弱性なし
12.4JDC	脆弱性なし
12.4JDD	脆弱性なし
12.4JDE	脆弱性なし
12.4JHA	脆弱性なし
12.4JHB	脆弱性なし
12.4JHC	脆弱性なし
12.4JK	脆弱性なし
12.4JL	脆弱性なし
12.4JX	脆弱性なし
12.4JY	脆弱性なし
12.4JZ	脆弱性なし
12.4MD	脆弱性あり。最初の修正はリリース12.4MDA 12.4(24)MDまでのリリースには脆弱性はありません。
12.4MDA	12.4(24)MDA13
12.4MDB	脆弱性あり。最初の修正はリリース12.4MDA
12.4MR	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
1240万	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4MRB	脆弱性あり。最初の修正はリリース15.1M
12.4SW	脆弱性あり。最初の修正はリリース15.1M
12.4T	脆弱性あり。最初の修正はリリース15.1M
12.4XA	脆弱性あり。最初の修正はリリース15.1M
12.4XB	脆弱性あり。最初の修正はリリース15.1M
12.4XC	脆弱性あり。最初の修正はリリース15.1M
12.4XD	脆弱性あり。最初の修正はリリース15.1M
12.4XE	脆弱性あり。最初の修正はリリース15.1M
12.4XF	脆弱性あり。最初の修正はリリース15.1M
12.4XG	脆弱性あり。最初の修正はリリース15.1M
12.4XJ	脆弱性あり。最初の修正はリリース15.1M
12.4XK	脆弱性あり。最初の修正はリリース15.1M
12.4XL	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4XM	脆弱性あり。最初の修正はリリース15.1M

12.4XN	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4XP	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4XQ	脆弱性あり。最初の修正はリリース15.1M
12.4XR	脆弱性あり。最初の修正はリリース15.1M
12.4XT	脆弱性あり。最初の修正はリリース15.1M
12.4XV	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4XW	脆弱性あり。最初の修正はリリース15.1M
12.4XY	脆弱性あり。最初の修正はリリース15.1M
12.4XZ	脆弱性あり。最初の修正はリリース15.1M
12.4YA	脆弱性あり。最初の修正はリリース15.1M
12.4YB	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4YD	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
12.4YE	脆弱性あり。最初の修正はリリース15.1M
12.4YG	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
影響を受ける 15.0 ベースのリリース	First Fixed Release（修正された最初のリリース）
15.0EA	脆弱性なし
15.0EB	脆弱性なし
15.0EC	脆弱性なし
15.0ED	脆弱性あり。15.2Eの任意のリリースに移行
15.0EF	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.0EH	脆弱性なし
15.0EJ	脆弱性なし
15.0EX	15.0(1)EX2
15.0EY	15.0(2)EY2
15.0EZ	15.0(1)EZ
15.0M	脆弱性あり。最初の修正はリリース15.1M
15.0MR	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.0秒	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。

15.0SE	15.0(2)SE3
15.0SG	15.0(2)SG7
15.0SQA	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.0SQB	脆弱性なし
15.0SY	15.0(1)SY5
15.0XA	脆弱性あり。最初の修正はリリース15.1M
15.0XO	脆弱性あり。最初の修正はリリース15.0SG
影響を受ける 15.1 ベースのリリース	First Fixed Release（修正された最初のリリース）
15.1EY	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.1GC	脆弱性あり。最初の修正はリリース15.1M
1,510万	15.1(4)M7
15.1MR	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.1MRA	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.1S	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.1SG	15.1(2)SG1
15.1SNG	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.1SNH	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.1SNI	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.1SVD	脆弱性なし
15.1SY	15.1(1)SY1 15.1(2)SY
15.1T	脆弱性あり。最初の修正はリリース15.1M
15.1XB	脆弱性あり。最初の修正はリリース15.1M
15.1XO	脆弱性なし
Affected 15.2-Based Releases	First Fixed Release（修正された最初のリリース）
15.2E	脆弱性なし
15.2EY	脆弱性なし
15.2GC	脆弱性あり。15.4Tの任意のリリースに移行

15.2JA	脆弱性なし
15.2JAX	脆弱性なし
15.2JB	15.2(2)JB2より前のリリースには脆弱性があり、15.2(2)JB2以降のリリースには脆弱性はありません。
15.2JN	脆弱性なし
1,520万	15.2(4)M4
15.2秒	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.2SA	15.2(2)SA
15.2SNG	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.2SNH	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
15.2SNI	脆弱性あり。最初の修正はリリース15.3S
15.2T	15.2(2)T4 15.2(3)T4
Affected 15.3-Based Releases	First Fixed Release（修正された最初のリリース）
15.3秒	15.3(1)S2 15.3(2)S1
15.3T	15.3(1)T2 15.3(2)T1 15.3(2)T2（2013年12月13日に入手可能）

Cisco IOS XE ソフトウェア

該当するリリース	First Fixed Release（修正された最初のリリース）
2.x	脆弱性あり、3.8.2S以降に移行
3.1.xSG	脆弱性あり、3.2.7SG以降に移行
3.2.xSG	3.2.7SG
3.2.xSE	3.2.2SE
3.2.xSQ	脆弱性あり、3.3.0SQ以降に移行
3.2.xXO	Vulnerable
3.3.xSG	脆弱性あり、3.4.1SGに移行
3.3.xSQ	脆弱性なし
3.4.xSG	3.4.1SG

3.1.xS	脆弱性あり、3.8.2S以降に移行
3.2.xS	脆弱性あり、3.8.2S以降に移行
3.3.xS	脆弱性あり、3.8.2S以降に移行
3.4.xS	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
3.5.xS	脆弱性あり、3.8.2S以降に移行
3.6.xS	脆弱性あり、3.8.2S以降に移行
3.7.xS	脆弱性が存在します。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください。
3.8.xS	3.8.2S
3.9.xS	3.9.1S
3.10.xS	脆弱性なし

Cisco ASAおよびCisco PIXソフトウェア

該当するリリース	First Fixed Release（修正された最初のリリース）
7.x	脆弱性あり、8.4.6.5以降に移行
8.0	脆弱性あり、8.4.6.5以降に移行
8.1	脆弱性あり、8.4.6.5以降に移行
8.2	脆弱性あり、8.4.6.5以降に移行
8.3	脆弱性あり、8.4.6.5以降に移行
8.4	8.4.6.5
8.5	脆弱性あり、9.0.3以降に移行
8.6	脆弱性あり、9.0.3以降に移行
8.7	脆弱性なし
9.0	9.0.3
9.1	9.1.2.5：このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織に連絡してください。

Cisco FWSMソフトウェア

Cisco FWSMソフトウェアのすべてのバージョンが、このドキュメントで説明されている脆弱性の影響を受けます。現在、Cisco.comには正式な修正済みリリースはありませんが、Cisco Technical Assistance Center(TAC)から暫定リリースを入手できます。

サービス契約をご利用のお客様は、このアドバイザリの「修正済みソフトウェアの入手」セクションの手順に従ってシスコのサポート部門にお問い合わせください。

Cisco NX-OS ソフトウェア

Cisco Nexus 7000:

該当するリリース	First Fixed Release（修正された最初のリリース）
4.(x)	Vulnerable
5.x	Vulnerable
6.0	Vulnerable
6.1	6.1(4)a
6.2	6.2.6
7.x	脆弱性なし

Cisco Nexus 5000:

該当するリリース	First Fixed Release（修正された最初のリリース）
4.(x)	Vulnerable
5.x	Vulnerable
6.x	Vulnerable
7.x	7.0.0.N1(1)

Cisco Nexus 3000、Cisco Nexus 4000、およびCisco Nexus 6000向けCisco NX-OSソフトウェアのすべてのバージョンが、このドキュメントで説明されている脆弱性の影響を受けます。現在、Cisco.comには正式な修正済みリリースはありませんが、Cisco Technical Assistance Center(TAC)から暫定リリースを入手できます。サービス契約をご利用のお客様は、このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従ってシスコのサポート組織にお問い合わせください。

Cisco StarOS ソフトウェア

この脆弱性は、Cisco StarOSソフトウェアバージョン14.0.50488で修正されています。

サービス契約をご利用のお客様は、このアドバイザリの「修正済みソフトウェアの入手」セクションの手順に従ってシスコのサポート部門にお問い合わせください。

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。

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。彼は、ベン・グリオン大学テレコム・イノベーション・ラボラトリーのEitan Menahem、Yuval Elovici、Ariel Waizelと共同で作業を行いました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130801-lsaospf

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.4	この脆弱性に該当しない製品のリストにCisco Nexus 9000を追加。	該当製品 – 脆弱性を含んでいないことが確認された製品	Final	2017年2月13日
1.3	付属のNX-OSソフトウェアテーブル			2014年7月31日
1.2	OVAL定義を含む			2013年8月17日
1.1	リンク切れを修正			2013年8月5日
1.0	初版リリース			2013年8月1日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者に

あるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な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。

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。