Cisco アグリゲーション サービス ルータ 900 のルート スイッチ プロセッサ 3 OSPFv2 で確認されたサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20190327-rsp3-ospf

初公開日 : 2019-03-27 16:00

バージョン 1.0 : Final

CVSSスコア : 7.4

回避策 : No workarounds available

Cisco バグ ID : CSCvh06656

CVE-2019-1749

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 アグリゲーション サービス ルータ（ASR）900 ルート スイッチ プロセッサ 3（RSP3）用の Cisco IOS XE ソフトウェアの入力トラフィック検証に含まれる脆弱性により、認証されていない隣接の攻撃者が、影響を受けるデバイスのリロードを引き起こし、その結果サービス妨害（DoS）状態を発生させる可能性があります。

この脆弱性は、RSP3 プラットフォームで使用される ASIC の入力トラフィックが十分に検証されないことに起因します。 攻撃者は、この脆弱性をエクスプロイトして、該当デバイスに不正な OSPF バージョン 2（OSPFv2）メッセージを送信することが可能です。 エクスプロイトに成功すると、攻撃者は、*iosd* プロセスのリロードを引き起こして該当デバイスのリロードを引き起こし、その結果 DoS 状態を発生させる可能性があります。

シスコはこの脆弱性に対処するソフトウェア アップデートをリリースしました。 この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-rsp3-ospf

このアドバイザリは、2019 年 3 月 27 日に公開された Cisco IOS ソフトウェアおよび IOS XE ソフトウェア リリースのセキュリティ アドバイザリ バンドルの一部です。このバンドルには、19 件の脆弱性に関して 17 件のシスコ セキュリティ アドバイザリが含まれています。 これらのアドバイザリとリンクの一覧については、以下を参照してください。シスコのイベント対応： Cisco

[IOS および IOS XE ソフトウェアに関するセキュリティ アドバイザリ公開資料（半年刊、2019 年 3 月）]

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOS XE ソフトウェアを実行していて、かつ OSPFv2 ルーティングおよび OSPF Message Digest 5（MD5）暗号認証機能が有効な Cisco ASR 900 RSP3 デバイスに影響を及ぼします。

注: OSPFv2 ルーティングおよびハッシュメッセージ認証コード セキュア ハッシュ アルゴリズム（HMAC-SHA）暗号化認証が有効なデバイスは、この脆弱性による影響を受けません。

脆弱性が存在する Cisco IOS XE ソフトウェア リリースについては、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ください。

OSPFv2 ルーティングが有効かどうかの確認

OSPFv2 ルーティングが有効かどうかは、**show running-config | include router ospf command** コマンドにより確認できます。 次に、OSPFv2 ルーティング機能が有効なデバイスからのコマンドの出力例を示します。

```
rsp3#show running-config | include router ospf
router ospf 1
```

このコマンドの出力が空の場合は、機能が設定されていないことを示します。

OSPF MD5 認証が設定されているかどうかの確認

OSPFv2 ルーティングが有効かどうかは、**show running-config | include authentication message-digest** コマンドを使用して、任意のデバイスで（またはグローバルに）OSPF MD5 認証が有効になっているかどうかを確認できます。 次に、1 つのインターフェイスで OSPF MD5 認証が有効になっているデバイスからのコマンドの出力の例を示します。

```
rsp3-1#show running-config | include authentication message-digest
 ip ospf authentication message-digest
```

次に、OSPF エリア 0 に関して OSPF MD5 認証がグローバルに有効になっているデバイスからのコマンドの出力の例を示します。

```
rsp3-2#show running-config | include authentication message-digest
 area 0authentication message-digest
```

このコマンドの出力が空の場合は、どのインターフェイスでも、またはグローバルにも、機能が有効になっていないことを示します。

Cisco IOS XE ソフトウェア リリースの判別

デバイス上で実行されている 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、CLI で **show version コマンド**を実行し、表示されるシステム バナーを参照することにより確認できます。 デバイスが Cisco IOS XE ソフトウェアを実行している場合、システム バナーに「*Cisco IOS Software*」、「*Cisco IOS XE Software*」などのテキストが表示されます。

次に、Cisco IOS XR ソフトウェア リリース 16.6.1 が実行されていて、インストールされているイメージ名が *PPC_LINUX_IOSD-UNIVERSALK9-M* であるデバイスでのコマンドの出力の例を示します。

```
rsp3-device# show version
Cisco IOS XE Software, Version 16.06.01
Cisco IOS Software [Everest], ASR900 Software (PPC_LINUX_IOSD-UNIVERSALK9-M), Version 16.6.1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Sat 22-Jul-17 03:12 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

シスコは、この脆弱性が Cisco IOS ソフトウェア、Cisco IOS XR ソフトウェア、および Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

回避策

この脆弱性に対処する回避策はありません。

Cisco IOS ソフトウェア リリース 15.4(1)T 以降でこの問題を軽減するには、暗号認証に MD5 アルゴリズムではなく HMAC-SHA アルゴリズムを使用するように OSPFv2 を設定します。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 HMAC-SHA を使用した暗号認証用の

OSPFv2 の設定の詳細については、『*IP Routing: OSPF Configuration Guide*』の「OSPFv2 Cryptographic Authentication」の章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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.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 TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/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

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の可能性を判断できるよう、シスコでは Cisco IOS Software Checker ツールを提供しています。このツールにより、特

定のソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。 また該当する場合、そのリリースに関するすべてのアドバイザリの脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

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 リストからリリース（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**、**3.13.8S** など）を入力します。

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。 「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[Impact Rating] ドロップダウン リストの [中間（Medium）] チェックボックスをオンにします。

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。

注: Cisco IOS XE ソフトウェア リリース 16.9.1 以降では、アップグレードにスマート ライセンスが必要です。 Cisco IOS XE をリリース 16.9.1 以降にアップグレードする予定がある場合は、スマート ライセンス要件を検討することをお勧めします。 次のドキュメントに追加情報が記載されています。 『Smart Licensing』

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 のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-rsp3-ospf

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019 年 3 月 27 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。