Cisco IOS および IOS XE ソフトウェアの IP サービス レベル契約で発見された、サービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20190327-ipsla-dos
初公開日 : 2019-03-27 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCvf37838

CVE-2019-1737

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 IOS ソフトウェアおよび Cisco IOS XE ソフトウェアによる IP サービス レベル契約（SLA）の処理に関する脆弱性により、認証されていないリモート攻撃者が該当デバイスにインターフェイス ウェッジを発生させ、Denial Of Service（DoS）状態を引き起こす可能性があります。

この脆弱性は、IP SLA レスポンダ アプリケーション コードによるソケット リソースの不適切な処理に起因します。細工された IP SLA パケットが攻撃者から該当デバイスに送信されると、エクスプロイトされる可能性があります。エクスプロイトに成功した場合、インターフェイス ウェッジが発生し、最終的にサービス妨害（DoS）状態を引き起こされる危険性があります。

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ています。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-ipsla-dos

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。アドバイザリとリンクの一覧については、『Cisco Event Response: March 2019 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

この脆弱性は、脆弱性が存在する特定リリースの Cisco IOS および IOS XE ソフトウェアを実行し、IP SLA レスポンダとして構成されているルータに影響を及ぼします。

脆弱性が存在する Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの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」の項を参照してください。

IP SLA 構成の確認

CLI コマンド show ip sla responder の出力結果が「Enabled」となるか確認することで、デバイスで IP SLA レスポンダが使用されているかどうかを調査できます。

次に、IP SLA レスポンダとして構成されているルータからのコマンド出力例を示します。

```
Router#show ip sla responder
                General IP SLA Responder on Control port 1967
                General IP SLA Responder on Control V2 port 1167
General IP SLA Responder is: Enabled
```

Cisco IOS 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 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 コマンドを使用し、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 ソフトウェアを実行している場合、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ます。バナーにはインストールされたイメージ名もカッコ内に表示され、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリース名が表示されます。一部のシスコ デバイスでは、show version コマンドをサポートしていなかったり、別の出力が表示されたりします。

次に、Cisco IOS ソフトウェア リリース 15.5(2)T1 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 C2951-UNIVERSALK9-M であるデバイスでのコマンド出力例を示します。

```
<#root>

Router>

show version

Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
.
.
.
```

Cisco IOS 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。

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 16.2.1 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 CAT3K_CAA-UNIVERSALK9-M であるデバイスでのコマンドの出力例を示します。

```
<#root>

ios-xe-device#

show version


Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali 16.2.1, REL
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 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のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が Cisco IOS XR ソフトウェアまたは 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。

詳細

キュー ウェッジは、Cisco IOS/IOS-XE ルータまたはスイッチで特定のパケットが受信されキューに入れられたものの、処理エラーのためキューから削除されないときに発生します。

キュー ウェッジの詳細や Cisco IOS ソフトウェアでブロックされたインターフェイスを特定するために使用できる検出方法については、このアドバイザリの「回避策」セクションを参照してください。また、シスコのセキュリティ ブログに記載されている「Cisco IOS Queue Wedges Explained」も参照してください。

セキュリティ侵害の痕跡

この脆弱性が不正利用されるデバイスでは、細工された IP SLA パケットは受信インターフェイスの入力キューでスタックし、結果的にそのキューがウェッジされます。インターフェイスがウェッジされると、ルータがリロードされるまでトラフィックの受信が停止します。

回避策

この脆弱性に対処する回避策はありません。

この脆弱性は、次の方法で識別できます。

組み込みイベント マネージャ

脆弱性のある Cisco IOS デバイス上で、Tool Command Language（TCL）に基づく組み込みイベント マネージャ（EEM）ポリシーを利用すると、この脆弱性によって引き起こされたインターフェイス キュー ウェッジを識別して、検出することができます。このポリシーによって、管理者は Cisco IOS デバイスのインターフェイスをモニタできるほか、インターフェイス入力キューがいっぱいになると、それを検出できます。Cisco IOS EEM がこの脆弱性による不正利用の可能性を検出すると、それに反応してポリシーがネットワーク管理者にアラートを送信し、それを受けて管理者は、入力キューをクリアするためにデバイスのアップグレード、適切な移行、またはリロードを行うことを判断できます。

Tclスクリプトは、次のリンクの「Cisco Beyond: Embedded Event Manager(EEM)Scripting Community」からダウンロードできます。 https://supportforums.cisco.com/docs/DOC-19337

詳細については、シスコのセキュリティ ブログに記載されている「 Cisco IOS Queue Wedges Explained」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。
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、[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 Cisco Service Contract 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 POS 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

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の可能性を判断するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、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。

	オン

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。スマートライセンスの詳細については、 こちらのドキュメントを参照してください。

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 Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-ipsla-dos

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2019 年 3 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。