Cisco IOSソフトウェア Wide Area Application Services Express サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20160323-l4f

初公開日 : 2016-03-23 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCuq59708

CVE-2016-1347

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ソフトウェアの Wide Area Application Services （ WAAS ） Express 機能の脆弱性はリモート攻撃者非認証により影響を受けたデバイスはリロードしますする可能性があります。

脆弱性は TCP セグメントの不十分な検証が原因です。 攻撃者は影響を受けたデバイスを通して巧妙に細工された TCP セグメントをルーティングすることによってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者により影響を受けたデバイスはリロードしますことを可能にする可能性がありまサービス拒否 （ DoS ）状態を引き起こします。

この脆弱性を不正利用するために、攻撃者は脆弱 な 機能がソフトウェアの出力 機能であるのでデバイスの出力 インターフェイスを通して巧妙に細工された TCP セグメントをルーティングする必要があります。 さらに、WAAS Express 機能はインターフェイスで一般的に WANインターフェイス 有効に する必要があります。 ほとんどの配備では、これは脆弱性を不正利用するために巧妙に細工された トラフィックがからデバイス中初期化する必要があることを意味します。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-l4f

このアドバイザリは、6 脆弱性を記述する 6 Cisco Security Advisory を含む Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書のリリースの 2016 年 3月 23 日一部です。 すべての脆弱性にあります「最高のセキュリティ へ の 影響 定格が」。 それらへの

アドバイザリおよびリンクの完全なリストに関しては、 Cisco イベント応答が表示されて下さい : 半年ごと Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書。

該当製品

小型に中間サイズのブランチ オフィスおよび遠隔地のために利用可能 な 帯域幅の量を増加する Cisco IOS WAAS Express 機能は WAN 最適化 ソリューションです、間 WAN 環境で動作する加速 TCP ベースのアプリケーション。 機能は WAN 最適化 ソリューションを提供するのに統合サービス ルータ（ISR）世代別 2 （G2）製品 グループと透過的に統合 Cisco IOSソフトウェアの機能を使用します。

脆弱性のある製品

この脆弱性は Cisco IOSソフトウェアの脆弱なリリースを実行して、1つ以上の WANインターフェイスで設定される WAAS Express がある Ciscoデバイスに影響を与えます。 Cisco IOS ソフトウェア リリースが脆弱である情報に関しては、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下さい。

WAAS Express 設定の査定

WAAS Express がインターフェイスで設定されるかどうか判別するために、管理者は **show running-config を**使用できます **| I waas イネーブル|^interface は**コマンドラインインターフェイスでまたは **waas status コマンドを示します。**

次の例は Ethernet0/1 インターフェイスで設定される WAAS Express があるルータの **show running-config コマンド**の出力を示したものです:

```
router#show running-config | i waas enable|^interface
.
.
.
interface Ethernet0/1
waas enable
.
.
.
```

次の例は Ethernet0/1 インターフェイスで設定される WAAS Express があるルータの **提示 waas status コマンド**の出力を示したものです:

```
router#show waas status
.
.
. WAAS Express Version: 2.0.0 WAAS Enabled Interface Policy Map Ethernet0/1 waas_global .
.
.
```

Cisco IOS ソフトウェア リリースの判別

、管理者はデバイスにログインどの Cisco IOS ソフトウェア リリースが Cisco製品で動作しているか判別し、**show version コマンドを**コマンドラインインターフェイスで使用し、次に現わ

れるシステムバナーを参照するためにできます。 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。 カッコ内にイメージ名が表示され、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することがあります。

次の例は、Cisco IOS ソフトウェア リリースが 15.5(2)T1 で、インストールされたイメージ名が *C2951-UNIVERSALK9-M* であるシスコ製品を示しています。

```
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ついては、以下を参照してください。[ホワイト ペーパー： Cisco IOS および NX-OS ソフトウェア リファレンス ガイド]

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 Cisco IOS XE ソフトウェア、Cisco IOS XR ソフトウェア、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。

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。
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場合は、http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、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 Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/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 ソフトウェア

顧客が Cisco IOSソフトウェアの脆弱性への公開を判別するのを助けるために Cisco はツールを、各アドバイザリに説明がある脆弱性を解決する以前のリリースおよび特定の Cisco IOS ソフトウェア リリースに影響を与える Cisco Security Advisory を識別する Cisco IOSソフトウェア チェッカー提供します、（「最初に」固定される）。 該当する場合、ツールはまた以前のリリースを戻します識別されるすべてのアドバイザリに説明があるすべての脆弱性を解決する（「結合される最初に」固定される）。

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含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全アドバイザリを含めるなど）を作成する

リリースがあらゆる公開された Cisco Security Advisory から影響を受けするかどうか判別するために、Cisco.com の Cisco IOSソフトウェア チェッカーを使用するか、または—次のフィールドで… Cisco IOS ソフトウェア リリースを—たとえば、**15.1(4)M2** 入力して下さい:

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

この問題は Cisco 内部テストの間に見つけられました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-l4f

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2016-March-23

利用規約