Cisco IOSソフトウェア リソース予約プロトコル（RSVP）インターフェイスキュー ウェッジ脆弱性

High

アドバイザリーID : cisco-sa-20130925-rsvp

初公開日 : 2013-09-25 16:00

最終更新日 : 2014-03-12 12:54

バージョン 1.1 : Final

CVSSスコア : 7.8

回避策 : Yes

Cisco バグ ID : CSCuf17023

CVE-2013-5478

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 ソフトウェアのリソース予約プロトコル（RSVP）機能の脆弱性はリモート攻撃者非認証が影響を受けたデバイスのインターフェイスキュー ウェッジを引き起こすようにする可能性があります。

脆弱性は UDP RSVP パケットの不適当な解析が原因です。 攻撃者は脆弱 な デバイスへ UDP ポート 1698 RSVP パケットを送信 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。 エクスプロイトにより Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェアは不正確にルーティング プロトコル 隣接関係の接続切断、損失、および他のサービス拒否（DoS）状態の原因となる場合があるインターフェイスキュー ウェッジに終って着信パケットを、処理します可能性があります。

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。

この脆弱性を軽減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。
925-rsvp

注： 2013 年 9月 25 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 8 Cisco Security Advisory が含まれています。 すべてのアドバイザリは Cisco IOSソフトウェアの脆弱性に対処します。 各 Cisco IOSソフトウェア Security Advisory は正しい 2013 年 9 月のすべ

ての Cisco IOSソフトウェア脆弱性はパブリケーションを組み込んだことアドバイザリ、また Cisco IOS ソフトウェア リリースで詳述される脆弱性を解決する Cisco IOS ソフトウェア リリースをリストします。

"Cisco Event Response: 半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクのパブリケーションを」組み込みました:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

該当製品

修正済みソフトウェア

特定のコンフィギュレーションのデバイスだけ影響を受けています。 影響を受けた Cisco IOSソフトウェアを実行するか、または Cisco IOS XE ソフトウェアによってがバージョン 脆弱である Ciscoデバイスはまた RSVP を有効に してもらう 1つ以上バーチャルルーティングおよびフォワーディング（VRF）インターフェイスをとき備え。 デバイスは次の条件の両方が満たされる場合脆弱です:

- 少なくとも 1 つの VRF 例は RSVP なしで設定されます
- 少なくとも 1 他に同じ VRF のインターフェイス（物理的か仮想 な）、ない（またはグローバル な 表にあります）、有効に なる RSVP があります

いくつかのシナリオ例は次の通りです:

- マルチプロトコル ラベル スイッチング（MPLS） インフラストラクチャで（RSVP-TE）設計する RSVP トラフィック
- 複数の VRF インフラストラクチャ
- VRF ライト インフラストラクチャ
- 有効に なる MPLS の Cisco 7600

デバイスが RSVP と、最もよいメソッド 有効に なる 天候を判別することは **提示 IP rsvp** コマンドラインインターフェイス exec （CLI）コマンドを使用することです。 デバイスが RSVP で設定されない場合、出力は RSVP が無効で、あらゆるインターフェイスで次の例に示すように有効に ならないことを示したものです:

```
Router#show ip rsvp
RSVP: disabled (not enabled on any interface)
```

デバイスが RSVP で設定されれば出力は RSVP が次の例に示すように有効に なることを示したものです:

```
Router#show ip rsvp
RSVP: enabled (on 1 interface(s))
```

注: Cisco 7600 ソフトウェア イメージは MPLS がデバイスで有効に なる場合内部 VLAN コンテキストの RSVP を有効に します。

デバイスへのトラフィック 誘導だけ脆弱性を引き起こします。 トランジットトラフィックは脆弱性を引き起こしません。 この脆弱性が UDP パケットを使用して不正利用することができ

るのでパケットの出典はスプーフィングされるかもしれません。

Cisco 製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、機器にログインし show version コマンドを実行してシステムバナーを表示させます。 "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 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_teamRouter> 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
```

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: http://www.cisco.com/web/about/security/intelligence/ios-ref.html の Cisco IOS および NX-OS ソフトウェア レファレンスガイド」。

脆弱性を含んでいないことが確認された製品

Cisco IOS XR ソフトウェアはこの脆弱性から影響を受けません。

Cisco IOS NX-OS ソフトウェアはこの脆弱性から影響を受けません。

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

リビジョン 1.1	2014-March-12	RSVP が有効に なったかどうか確認を助けるべき「該当製品」セクションの追加された追加詳細。
リビジョン 1.0	2013-September-25	初版リリース

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。