Cisco IOSソフトウェアのRSVP脆弱性

アドバイザリーID : cisco-sa-20140924-rsvp CVE-2014-3354
初公開日 : 2014-09-24 16:00
最終更新日 : 2014-09-26 19:15
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCui11547

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Resource Reservation Protocol(RSVP)の実装における脆弱性により、認証されていないリモートの攻撃者がデバイスのリロードを引き起こす可能性があります。この脆弱性が繰り返し悪用されると、長時間にわたってサービス拒否(DoS)状態が発生す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ています。

この脆弱性に対しては回避策があります。

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-20140924-rsvp

注： 2014年9月24日の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には6件の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ています。個々の公開リンクは、次のリンクにある『Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication』に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep14.html

該当製品

脆弱性のある製品

Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアでRSVPプロトコルの使用が有効になっているデバイスは、この脆弱性の影響を受けます。

デバイスでRSVPが有効になっているかどうかを確認するには、次の2つの方法があります。

- デバイスでRSVPがアクティブかどうかを確認します。
- デバイスの設定にRSVPコマンドが含まれているかどうかを確認します。

Cisco IOSデバイスでRSVPが有効になっているかどうかを確認するには、デバイスでRSVPが有効になっているかどうかを確認することをお勧めします。

デバイスでRSVPがアクティブかどうかの確認

管理者は、 show ip rsvp interface showコマンドを使用して、Cisco IOSデバイスでRSVPが有効になっているかどうかを確認できます。影響を受けるデバイスでは、コマンドの出力に少なくとも1つのインターフェイスが含まれます。次の例は、RSVPプロトコルがアクティブになっているデバイスを示しています。

<#root>

```
Router>

show ip rsvp interface

interface    rsvp  allocated  i/f max  flow max sub max  VRF
Gi0/1        ena   0          100K     100K     0
Router>
```

次の例は、RSVPプロトコルがどのルータインターフェイスでもアクティブでないデバイスを示しており、そのデバイスは脆弱ではありません。

<#root>

```
Router>

show ip rsvp interface

interface    rsvp  allocated  i/f max  flow max sub max  VRF
Router>
```

デバイス設定にRSVPコマンドが含まれているかどうかの確認

RSVPプロトコルを使用するように設定されているデバイスは、この脆弱性の影響を受けます。Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアデバイスでRSVPが設定されているかどうかを確認するには、管理者がCLIで show running | include rsvp bandwidth|mpls traffic-eng tunnelコマンドを使用します。該当するデバイスには、 ip rsvp bandwidthインターフェイス設定コマンドまたは mpls traffic-eng tunnelインターフェイス設定コマンドが少なくとも1回は含まれます。

次の例は、RSVPプロトコルがアクティブになっているデバイスを示しています。

<#root>

```
Router#

show running | include rsvp|mpls traffic-eng tunnel

 ip rsvp bandwidth 100
 ip rsvp bandwidth 100
 mpls traffic-eng tunnel
Router#
```

Cisco IOSソフトウェアリリースの判別

シスコ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、デバイスにログインして show version コマンドを使って、システム バナーを表示します。"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、Cisco IOS ソフトウェア リリースが 15.2(4)M5、インストールされたイメージ名が C3900-UNIVERSALK9-M であるシスコ製品を示しています。

```
<#root>

Router>

show version

Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), 15.2(4)M5, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 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、『White Paper: Cisco IOS and NX-OS Software Reference Guide』で確認できます。

脆弱性を含んでいないことが確認された製品

次の製品は、この脆弱性の影響を受けません。

- Cisco NX-OS ソフトウェア
- Cisco IOS XR ソフトウェア

- Cisco ASA ソフトウェア

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

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアには、RSVPプロトコルで設定された場合に脆弱性が存在します。この脆弱性により、認証されていないリモートの攻撃者がデバイスのリロードを引き起こす可能性があります。この脆弱性が繰り返し悪用されると、長時間にわたってDoS状態が発生する可能性があります。

RSVPプロトコルが設定されているデバイスには脆弱性が存在します。影響を受けるインフラストラクチャの知識を持つ攻撃者は、脆弱性のあるデバイスに不正なIPv4またはIPv6 RSVPパケットをUDPポート1698またはIPプロトコル46経由で送信することで、この脆弱性を不正利用する可能性があります。この脆弱性は、デバイス宛てのトラフィックまたは通過トラフィックによって不正利用される可能性があります。他のRSVP UDPポート、TCPポート、またはIPプロトコルは影響を受けません。この脆弱性の不正利用に成功すると、攻撃者がデバイスをリロードできる可能性があります。

この脆弱性は、デバイス宛てのトラフィックまたは通過トラフィックによって不正利用される可能性があります。この脆弱性が不正利用されるのは、RSVPが有効になっているインターフェイスで不正なパケットがルータに着信した場合だけです。

この脆弱性を軽減する回避策があります。

この脆弱性は、Cisco Bug ID CSCui11547(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2014-3354が割り当てられています。

回避策

この脆弱性に対しては、次の緩和策があります。

コントロール プレーン ポリシング

IPv4での緩和策として、コントロールプレーンポリシング(CoPP)を使用して、ポート1698およびIPプロトコル46で信頼できないUDPトラフィックをブロックできます。Cisco IOS ソフトウェア リリース 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T は、CoPP 機能をサポートしています。CoPPをデバイスに設定して、管理プレーンとコントロールプレーンを保護し、既存のセキュリティポリシーと設定に従ってインフラストラクチャデバイスに送信される承認されたトラフィックのみを明示的に許可することで、インフラストラクチャへの直接攻撃のリスクと効果を最小限に抑えることができます。次のCoPPの例は、インフラストラクチャIPアドレスの範囲内にあるIPアドレスを持つすべてのデバイスを保護するために導入されるCoPPの一部として含める必

要があります。

```
!--- Feature: RSVP

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD any eq 1698
access-list 150 deny 46 TRUSTED_SOURCE_ADDRESSES WILDCARD any

!--- Deny RSVP over UDP traffic from all other sources destined
!--- to the device control plane.

access-list 150 permit udp any any eq 1698
access-list 150 permit 46 any any

!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all drop-udp-class
  match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-udp-traffic
  class drop-udp-class
  drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
  service-policy input drop-udp-traffic
```

前記のCoPPの例では、アクセスコントロールリストエントリ(ACE)の permitアクションに一致する潜在的な悪用パケットがある場合、これらのパケットはポリシーマップの drop機能によって廃棄されますが、 denyアクション（非表示）に一致するパケットは、ポリシーマップの drop機能の影響を受けません。policy-mapの構文は、12.2Sと12.0SのCisco IOSソフトウェアトレインでは異なることに注意してください。

```
policy-map drop-udp-traffic
class drop-udp-class police 32000 1500 1500 conform-action drop exceed-action
drop
```

CoPPは、IPv6を介した攻撃に対する効果的な緩和策ではありません。

CoPP機能の設定と使用についての詳細は、次のリンクの『 Control Plane Policing Implementation Best Practices』および『 Control Plane Policing』に記載されています。
http://www.cisco.com/web/about/security/intelligence/coppwp_gs.htmlおよび
http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/htcpp.html

修正済みソフトウェア

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 のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の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

シスコは、お客様がCisco IOSソフトウェアの脆弱性の影響を受けるかどうかを判断するためのツールを提供しています。 Cisco IOS Software Checker により、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を選択するか、ローカル システムからファイルをアップロードすることによって、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を作成して、以前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、特定の資料、または2015年9月のバンドル資料のすべてのアドバイザリを含めます

このツールは、クエリされたソフトウェアリリースに影響を与えるシスコセキュリティアドバイザリと、各シスコセキュリティアドバイザリのすべての脆弱性を修正する最初のリリース(First Fixed)を特定します。該当する場合、表示されたすべてのアドバイザリのすべての脆弱性を修正する最初のリリース(Combined First Fixed)も返します。Cisco IOS Software Checkerにアクセスするか、次のフィールドにCisco IOSソフトウェアリリースを入力して、このバンドルアドバイザリアドバイザリの影響を受受受えないかどうかを判断します。

(例：15.1(4)M2)

Check

Cisco IOS XE ソフトウェア

Cisco IOS XEソフトウェアは、このアドバイザリに記載されている脆弱性の影響を受けます。

Cisco IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）	2014年9月の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に含まれるすべてのアドバイザリに対する最初の修正リ

		リース
2.1.x	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.6S以降に移行してください。
2.2.x	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.6S以降に移行してください。
2.3.x	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.6S以降に移行してください。
2.4.x	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.6S以降に移行してください。
2.5.x	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.6S以降に移行してください。
2.6.x	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.6S以降に移行してください。
3.1.xS	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.6S以降に移行してください。
3.1.xSG	脆弱性なし	脆弱性なし
3.2.xS	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.6S以降に移行してください。
3.2.xSE	脆弱性あり、3.3.2SEに移行	脆弱性あり、3.3.2SEに移行
3.2.xSG	脆弱性なし	脆弱性なし
3.2.xXO	脆弱性なし	脆弱性なし
3.2.xSQ	脆弱性なし	脆弱性なし
3.3.xS	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.6S以降に移行してください。
3.3.xSE	3.3.2SE	3.3.2SE

3.3.xSG	脆弱性あり。 3.4.4SG以降に移行してください。	脆弱性あり。3.4.4SG以降に移行してください。
3.3.xXO	脆弱性なし	3.3.1XO
3.3.xSQ	脆弱性なし	脆弱性なし
3.4.xS	3.7.4S	脆弱性あり。3.7.6S以降に移行してください。
3.4.xSG	3.4.4SG	3.4.4SG
3.4.xSQ	脆弱性なし	脆弱性なし
3.5.xS	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.6S以降に移行してください。
3.5.xE	脆弱性なし	3.5.2E
3.6.xS	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.6S以降に移行してください。
3.6.xE	脆弱性なし	脆弱性なし
3.7.xS	3.7.4S	脆弱性あり。3.7.6S以降に移行してください。
3.7.xE	脆弱性なし	脆弱性なし
3.8.xS	脆弱性あり。 3.10.1S以降に移行してください。	脆弱性あり。3.10.4S以降に移行してください。
3.9.xS	脆弱性あり。 3.10.1S以降に移行してください。	脆弱性あり。3.10.4S以降に移行してください。
3.10.xS	3.10.1S	3.10.4S
3.11.xS	脆弱性なし	脆弱性あり。3.12S以降に移行してください。
3.12.xS	脆弱性なし	脆弱性なし
3.13.xS	脆弱性なし	脆弱性なし

Cisco IOS ソフトウェア リリースへの Cisco IOS XE ソフトウェア リリースのマッピングについては、「 Cisco IOS XE 2 Release Notes」、「 Cisco IOS XE 3S Release Notes」、および「 Cisco IOS XE 3SG Release Notes」を参照してください。

Cisco IOS XR ソフトウェア

Cisco IOS XRソフトウェアは、2014年9月のCisco IOS Software Security Advisoryバンドル公開に含まれている脆弱性の影響を受けません。

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、シスコ内部でのセキュリティテストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-rsvp

改訂履歴

リビジョン 1.1	2014年9月 26日	MPLS-TEトンネルに関する説明を追加。
リビジョン 1.0	2014年9月 24日	初回公開リリース

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。