Cisco IOS Software RSVP Vulnerability

Advisory ID: cisco-sa-20140924-rsvp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-rsvp

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。

Revision 1.0

For Public Release 2014 September 24 16:00 UTC (GMT)

目次

要約

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）を実装する際の脆弱性により、認証されていないリモートの攻撃者によってデバイスがリロードさせられる可能性があります。またこの脆弱性が繰り返し不正利用されると、長時間にわたってサービス拒否（DoS）状態が続きます。

シスコはこの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ました。

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、次のリンクで確認できます。
http://tools.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。これらのアドバイザリはすべて、Cisco IOS ソフトウェアの脆弱性に対処するものです。個別の公開リンクは、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/cisco/web/support/JP/112/1126/1126235_Cisco_ERP_sep14-j.html

該当製品

脆弱性が認められる製品

Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアで RSVP プロトコルを使用するように設定されたデバイスは、この脆弱性の影響を受けます。

デバイスに RSVP が設定されているかどうかは、次の 2 つの方法で確認できます。

- デバイスで RSVP が有効か確認する。
- デバイスの設定に RSVP コマンドが含まれているか確認する。

Cisco IOS デバイスで RSVP が有効になっているかどうかを調べるには、デバイスで RSVP が有効かどうか確認することを推奨します。

デバイスで RSVP が有効か確認する

管理者は **show ip rsvp | include RSVP: enabled** show コマンドを使用して Cisco IOS デバイスで RSVP が有効か確認することができます。有効になっているデバイスでは、コマンドの出力に **RSVP: enabled** が含まれます。次の例は、RSVP プロトコルが有効になっているデバイスでの表示例です。

```
Router> show ip rsvp | include RSVP: enable
RSVP: enabled (on 1 interface(s))
Router>
```

デバイスの設定に RSVP コマンドが含まれているか確認する

Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアの設定において RSVP が有効になっているかどうかは、少なくとも 1 つの **ip rsvp bandwidth** インターフェイス コンフィギュレーション コマンドが設定に存在していることで確認できます。 **show running | include rsvp** コマンドです。RSVP が有効になっているデバイスでは、 **ip rsvp bandwidth** インターフェイス設定コマンドが少なくとも 1 つ存在します。次の例は、RSVP プロトコルが設定されているデバイスでの表示例です。

```
Router# show running | include rsvp
 ip rsvp bandwidth 100
 ip rsvp bandwidth 100
Router#
```

Cisco IOS ソフトウェア リリースを確認する

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 **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、続いてバージョンと Cisco IOS ソフトウェア 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** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で Cisco IOS ソフトウェア リリース 15.2(4)M5 が稼働し、インストールされているイメージ名が C3900-UNIVERSALK9-M であることを示しています。

```
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_teamRouter> 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
```

Cisco IOS ソフトウェア リリースの命名規則の追加情報は、ホワイト ペーパー「Cisco IOS and NX-OS Software Reference Guide」で確認できます。

脆弱性が認められない製品

次の製品または機能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、この脆弱性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 プロトコルを設定した場合に脆弱性が生じます。この脆弱性により、認証されていないリモートの攻撃者によってデバイスがリロードさせられる可能性があります。またこの脆弱性が繰り返し不正利用されることにより、長時間にわたって DoS 状態が続きます。

RSVP プロトコルを設定するとデバイスに脆弱性が生じます。この脆弱性の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、UDP ポート 1698 を介して脆弱性を持つデバイスに不正な IPv4 または IPv6 RSVP パケットを送信し、この脆弱性を不正利用する可能性があります。この脆弱性の不正利用には、デバイス宛てのトラフィックとデバイスを通過するトラフィックのいずれも使用できます。その他の 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。この脆弱性が不正利用されると、攻撃者によってデバイスがリロードさせられる可能性があります。

この脆弱性の不正利用には、デバイス宛てのトラフィックとデバイスを通過するトラフィックのいずれも使用できます。

この脆弱性に対しては回避策があります。

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。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助

けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。
http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。
http://tools.cisco.com/security/center/cvssCalculator.x

CSCui11547 Cisco IOS RSVP Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性が不正利用されると、該当するデバイスがリロードさせられる可能性があります。

ソフトウェア バージョンおよび修正

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, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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

シスコでは、Cisco IOS ソフトウェアの脆弱性を判断するためのツールを提供しています。Cisco IOS ソフトウェア チェッカーを使用すると、お客様は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

をアップロードして、検索を開始する。
- **show version** コマンド出力を入力してツールで解析する。
- 以前に公開されたすべての Cisco Security Advisory、特定の公開内容、または 2014 年 9 月のすべてのバンドル公開内容を含めて、カスタマイズされた検索を作成する。

このツールにより、クエリされたソフトウェア リリースに影響を与える Cisco Security Advisory と、各 Cisco Security Advisory のすべての脆弱性を修正する最初のリリース（初回修正）を見つけることができます。このツールはさらに、表示された全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（総合初回修正）も返します。Cisco IOS ソフトウェア チェッカーを使用するか、または以下のフィールドに Cisco IOS ソフトウェアのリリースを入力し、このバンドル公開に含まれているいずれかのアドバイザリの影響を受けるものがあるかどうかを判断してください。

（入力例：15.1(4)M2）

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 Software Release	First Fixed Release	First Fixed Release for All Advisories in the September 2014 Cisco IOS Software Security Advisory Bundled Publication
2.1.x	Vulnerable; migrate to 3.7.4S or later.	Vulnerable; migrate to 3.7.6S or later.
2.2.x	Vulnerable; migrate to 3.7.4S or later.	Vulnerable; migrate to 3.7.6S or later.
2.3.x	Vulnerable; migrate to 3.7.4S or later.	Vulnerable; migrate to 3.7.6S or later.
2.4.x	Vulnerable; migrate to 3.7.4S or later.	Vulnerable; migrate to 3.7.6S or later.
2.5.x	Vulnerable; migrate to 3.7.4S or later.	Vulnerable; migrate to 3.7.6S or later.
2.6.x	Vulnerable; migrate to 3.7.4S or later.	Vulnerable; migrate to 3.7.6S or later.
3.1.xS	Vulnerable; migrate to 3.7.4S or later.	Vulnerable; migrate to 3.7.6S or later.
3.1.xSG	Not vulnerable	Not vulnerable
3.2.xS	Vulnerable; migrate to 3.7.4S or later.	Vulnerable; migrate to 3.7.6S or later.
3.2.xSE	Vulnerable;	Vulnerable; migrate to 3.3.2SE

	migrate to 3.3.2SE	
3.2.xSG	Not vulnerable	Not vulnerable
3.2.xXO	Not vulnerable	Not vulnerable
3.2.xSQ	Not vulnerable	Not vulnerable
3.3.xS	Vulnerable; migrate to 3.7.4S or later.	Vulnerable; migrate to 3.7.6S or later.
3.3.xSE	3.3.2SE	3.3.2SE
3.3.xSG	Vulnerable; migrate to 3.4.4SG or later.	Vulnerable; migrate to 3.4.4SG or later.
3.3.xXO	Not vulnerable	3.3.1XO
3.3.xSQ	Not vulnerable	Not vulnerable
3.4.xS	3.7.4S	Vulnerable; migrate to 3.7.6S or later.
3.4.xSG	3.4.4SG	3.4.4SG
3.4.xSQ	Not vulnerable	Not vulnerable
3.5.xS	Vulnerable; migrate to 3.7.4S or later.	Vulnerable; migrate to 3.7.6S or later.
3.5.xE	Not vulnerable	3.5.2E
3.6.xS	Vulnerable; migrate to 3.7.4S or later.	Vulnerable; migrate to 3.7.6S or later.
3.6.xE	Not vulnerable	Not vulnerable
3.7.xS	3.7.4S	Vulnerable; migrate to 3.7.6S or later.
3.7.xE	Not vulnerable	Not vulnerable
3.8.xS	Vulnerable; migrate to 3.10.1S or later.	Vulnerable; migrate to 3.10.4S or later.
3.9.xS	Vulnerable; migrate to 3.10.1S or later.	Vulnerable; migrate to 3.10.4S or later.
3.10.xS	3.10.1S	3.10.4S
3.11.xS	Not vulnerable	Vulnerable; migrate to 3.12S or later.
3.12.xS	Not vulnerable	Not vulnerable
3.13.xS	Not vulnerable	Not vulnerable

Cisco IOS XE ソフトウェア リリースの Cisco IOS ソフトウェア リリースへのマッピングについては、『Cisco IOS XE 2 リリース ノート』、『Cisco IOS XE 3S リリース ノート』、『Cisco IOS XE 3SG リリース ノート』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。

回避策

この脆弱性に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、信頼できない UDP トラフィックがデバイスに進入するのをブロックすることができます。CoPP 機能は、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 でサポートされています。管理およびコントロール プレーンを保護するために CoPP をデバイスに設定し、既存のセキュリティ ポリシーと設定に従って認定されたトラフィックだけがインフラストラクチャ デバイス宛てに送信されること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その効果を最小限に抑えることができます。下記の 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定義される CoPP の一部として含む必要がある項目です。

```
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
```

上記の CoPP の例では、 **permit** アクションによって、アクセス コントロール リスト エントリ（ACE）に該当する攻撃の可能性のあるパケットを照合し、policy-map の **drop** 機能でそれらのパケットが廃棄されますが、その一方、 **deny** アクション（記載されていません）に該当するパケットは、policy-map の **drop** 機能の影響を受けません。policy-map の構文は、12.2S と 12.0S Cisco IOS ソフトウェア トレインでは異なるので注意が必要です。

```
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
```

CoPP は、IPv6 を介した攻撃に対しては有効な緩和策ではありません。

コントロール プレーン ポリシング（CoPP）機能の設定および使用に関する詳細は、「コントロール プレーン ポリシングの実装に関するベスト プラクティス」（ http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html ）および「コントロール プレーン ポリシング」（ http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/htcpp.html ）に記載されています。

修正済みソフトウェアの入手

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。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

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、ご購入いただいたフィーチャ 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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、 Cisco.com の Software Navigator からアップグレードを入手することができます。 http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- Eメール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（ http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html ）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）では、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とその公表は確認しておりません。

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たものです。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-rsvp

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2014-September-24	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。この Web ページには、Cisco Security Advisory に関してメディアが問い合わせる際の指示が掲載されています。すべての Cisco Security Advisory は、 http://www.cisco.com/go/psirt/ で確認することができます。