Cisco IOSソフトウェアメタデータの脆弱性

アドバイザリーID : cisco-sa-20140924-metadata
初公開日 : 2014-09-24 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 : CSCue22753 CSCug75942

CVE-2014-3356
CVE-2014-3355

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ソフトウェアのメタデータフロー機能における2つの脆弱性により、認証されていないリモートの攻撃者によって脆弱なデバイスがリロードされる可能性があります。

この脆弱性は、メタデータインフラストラクチャで処理する必要があるトランジットRSVPパケットの不適切な処理に起因します。攻撃者は、不正な形式のRSVPパケットを該当デバイスに送信することで、これらの脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は拡張サービス拒否(DoS)状態を引き起こす可能性があります。

シスコはこれら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。

これらの脆弱性を軽減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-20140924-metadata

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

メタデータフロー機能を使用するように設定されているデバイスは、これらの脆弱性の影響を受けます。メタデータフローがIOSデバイスで設定されているかどうかを確認するには、管理者がNX-OS CLIで show running | include metadataコマンドを使用します。該当するデバイスには、 metadata flowコマンドが含まれます。コマンドには、グローバルコンフィギュレーションモード用とインターフェイスコンフィギュレーションモード用の2種類のバリエーションがあります。どちらのコマンドを使用した場合も、デバイスに脆弱性が生じます。

次の例は、メタデータ機能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 metadata

 metadata flow
Router#
```

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、このドキュメントで説明されている脆弱性の影響を受けないことが確認されています。

- Cisco NX-OS ソフトウェア
- Cisco IOS XR 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

メタデータインフラストラクチャは、ネットワーク要素上で確認されるネットワークフローからのデータを、同じネットワーク要素上の別のコンポーネントおよびネットワーク要素間で使用できるようにするフレームワークを提供します。フローメタデータは、ネットワーク内のフローを記述するデータです。RSVPフローなどのフローは、シグナリングが検査され、コントロールプレーンデータベースと呼ばれるデータベースにその属性が格納されます。

このドキュメントの脆弱性は、メタデータが制御データベースに保存される際の、メタデータ機能による特定のRSVPフローの処理に関連しています。脆弱性を引き起こすRSVPフローは、脆弱性を含むデバイス宛てのものではなく、通過トラフィックです。

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアにメタデータフロー機能が設定されている場合、2つの脆弱性が存在します。これらの脆弱性により、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。これら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。

メタデータフロー機能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、IPプロトコル46およびIPプロトコル134で特定の不正なRSVPパケットを送信することにより、これらの脆弱性を不正利用する可能性があります。UDPポートまたはTCPポートは、これらの脆弱性の影響を受けません。

15.3(1)TでのIPv6を介したメタデータフローの統合から、この脆弱性はIPv6でも不正利用される可能性があります(Cisco Bug ID CSCtw57401を参照)。脆弱性のあるデバイスがIPv6機能を介したメタデータをサポートしているかどうかを確認するには、 show metadata flow table ipv6 execコマンドを使用します。IPv6を介したメタデータをサポートするデバイスでは、次の出力が生成されます。
<#root>

```
Router>
```

```
show metadata flow table ipv6

To                                    From
Flow  Proto DPort SPort Ingress      Egress

Router>
```

これらの脆弱性が悪用されると、攻撃者は該当するデバイスをリロードする可能性があります。

これらの脆弱性を軽減する回避策はありません。

これらの脆弱性は、Cisco Bug ID CSCue22753(登録ユーザ専用)と CSCug75942(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-2014-3356とCVE-2014-3355がそれぞれ5が5割3として定められています。

回避策

回避策はありません。

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

シスコでは、お客様がCisco IOSソフトウェアの脆弱性による影響を受ける可能性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の作成 (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るか、特定の資料を対象にするか、2015年9月のバンドル資料のすべてのアドバイザリを対象とする)

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 (以下

「最初の修正」）を特定します。また、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（以下「最初の修正」）も特定します。Cisco IOS Software Checkerにアクセスするか、以下のフィールドに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のいずれかに該当該当するかどうかを判断してください。

(入力例：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の最初の修正リリース
2.1.x	脆弱性なし	脆弱性あり。3.7.6S以降に移行してください。
2.2.x	脆弱性なし	脆弱性あり。3.7.6S以降に移行してください。
2.3.x	脆弱性なし	脆弱性あり。3.7.6S以降に移行してください。
2.4.x	脆弱性なし	脆弱性あり。3.7.6S以降に移行してください。
2.5.x	脆弱性なし	脆弱性あり。3.7.6S以降に移行してください。
2.6.x	脆弱性なし	脆弱性あり。3.7.6S以降に移行してください。
3.1.xS	脆弱性なし	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	脆弱性なし	脆弱性あり。3.7.6S以降に移行してください。
3.2.xSE	脆弱性なし	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	脆弱性なし	脆弱性あり。3.7.6S以降に移行してください。
3.3.xSE	脆弱性なし	3.3.2SE
3.3.xSG	脆弱性なし	脆弱性あり。3.4.4SG以降に移行してください。
3.3.xXO	3.3.1XO	3.3.1XO
3.3.xSQ	脆弱性なし	脆弱性なし
3.4.xS	脆弱性なし	脆弱性あり。3.7.6S以降に移行してください。
3.4.xSG	脆弱性なし	3.4.4SG
3.4.xSQ	脆弱性なし	脆弱性なし
3.5.xS	脆弱性なし	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。3.7.6S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	3.7.6S	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。 3.10.4S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。 3.10.4S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	3.10.4S	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）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。

これらの脆弱性は、シスコの社内テストで発見されたものです。

URL

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

改訂履歴

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。