Cisco IOSソフトウェア メタデータ脆弱性

High

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

メタデータ機能の 2 脆弱性は Cisco IOSソフトウェアの非認証が脆弱なデバイスをリロードするようにする可能性がありますリモート攻撃者フローします。

脆弱性はメタデータ インフラストラクチャによって処理される必要がある中継 RSVP パケットの不適当な処理が原因です。 攻撃者は影響を受けたデバイスへ形式が間違った RSVP パケットを送信 することによってこれら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拡張サービス拒否 （DoS）状態を引き起こすことを可能にする可能性があります。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。

これらの脆弱性を軽減する回避策は利用できません。

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-20140924-metadata

注: 2014 年 9月 24 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 6 Cisco Security Advisory が含まれています。 すべての状況報告は Cisco IOSソフトウェアの脆弱性に対処します。 個々の公表資料へのリンクは、次のリンクにある「*シスコのイベント対応：半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクで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_sep14.html

該当製品

脆弱性のある製品

メタデータを機能使用するために設定されるデバイスはこれらの脆弱性から影響を受けますフローします。 メタデータがフローするかどうか判別することは IOSデバイスで、管理者 **show running を**使用できます設定されました **| メタデータ** コマンドを **含んで下さい**。 影響を受けたデバイスは **メタデータが**コマンド **フローします**含まれています。 コマンドの 2 つのバリエーション、インターフェイス設定モードにおけるグローバル コンフィギュレーション モードのための 1 および別のものがあります。 コマンドのどちらかの変化はデバイスを脆弱にします。

次の例はメタデータ機能がアクティブであるデバイスを示したものです:

```
Router# show running | include metadata
 metadata flow
Router#
```

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 "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。

```
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
```

```
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
```

Cisco IOS ソフトウェア リリースの命名規則については、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

以下の製品はこの文書に説明がある脆弱性に脆弱ではないために確認されませんでした:

- 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同じネットワーク要素のおよび Network Elements を渡る別のコンポーネントに利用可能であるためにネットワーク要素で見られるネットワーク 流 れからのデータを可能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でフローを記述するデータです。 RSVP フローのようなフローはデータベースで属性を保存する信号を送ることのためにコントロール プレーン データベースとして参照されて点検されます。

この文書の脆弱性はメタデータ機能によってある特定の RSVP フローの処理とメタデータが制御データベースで保存される筈であるとき関連しています。 脆弱性を引き起こす RSVP フローは脆弱なデバイスに宛先としないでが、脆弱なデバイスによって見られるようにトランジットトラフィックです。

メタデータ機能で設定されたとき Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェアは 2 脆弱性がフローします含まれています。 これらの脆弱性はリモート攻撃者非認証によりデバイスのリロードを引き起こすようにする可能性があります。 これらの脆弱性が拡張 DoS 状態を引き起こすのに繰り返し不正利用できます。

デバイスはメタデータ機能でフローすれば設定される場合脆弱です。 影響を受けたインフラストラクチャのナレッジの攻撃者は IP プロトコル 46 および IP プロトコル 134 のある特定の形式が間違った RSVP パケットの送信によってこれらの脆弱性を不正利用する可能性があります。 UDP または TCP ポートはこれらの脆弱性から影響を受けません。

メタデータの統合から開始して、脆弱性は 15.3(1)T で IPv6 にまた IPv6 によって不正利用することができますフローします（Cisco バグ ID CSCtw57401 を参照して下さい）。 IPv6 上のメタデータが特色にする脆弱なデバイスサポートかどうか判別するために、 **提示メタデータを** EXEC コマンド **フローします表 IPv6** 使用して下さい。 IPv6 上のメタデータをサポートするデバイスは次の出力を生成 します:

```
Router> show metadata flow table ipv6
To                                    From
Flow  Proto DPort SPort Ingress       Egress

Router>
```

これらの脆弱性の不正利用の成功は攻撃者が脆弱なデバイスをリロードすることを可能にする可能性があります。

回避策はこれらの脆弱性を軽減して利用できません。

これらの脆弱性 Cisco バグ ID CSCue22753 （ 登録ユーザのみ ）および CSCug75942 （ 登録ユーザのみ ）で文書化されています、よくある脆弱性および公開（CVE） ID CVE-2014-3356 およ

び CVE-2014-3355 は、それぞれ割り当てられました。

回避策

対応策は見つかりません。

修正済みソフトウェア

ソフトウェアアップグレードを検討するとき、顧客は Cisco Security Advisory、応答および表記アーカイブを http://www.cisco.com/go/psirt で参照し、公開および完全なアップグレード ソリューションを判別するためにそれに続く状況報告を検討するように勧告されます。

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

Cisco は顧客が 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ようにツールを提供しました。 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
- 2015 年 9 月組み込まれた書にすべての以前に公開された Cisco Security Advisory、特定のパブリケーション、またはすべての状況報告を含めることによってカスタマイズされた検索を作成して下さい

ツールは問い合わせられたソフトウェア リリースおよび各 Cisco Security Advisory のすべての脆弱性を解決する以前のリリースに影響を与える Cisco Security Advisory を識別します（「最初に」固定される）。 該当する場合、ツールはまたすべての表示された状況報告のすべての脆弱性を解決する最も早い可能性のあるリリースを戻します（「結合される最初に」固定される）。 Cisco IOSソフトウェア チェッカーを単に参照するか、または次のフィールドでこの組み込まれたパブリケーションの状況報告の何れかから影響を受けるかどうか判別するために Cisco IOS ソフトウェア リリースを入力して下さい。

（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状況報告に説明がある脆弱性から影響を受けます。

Cisco	First Fixed Release（修	2014 年 9 月 Cisco IOSソフトウェア Security

IOS XE ソフトウェアリリース	正された最初のリリース）	Advisory によって組み込まれる書のすべてのアドバイザリーのための最初修正済みリリース
2.1.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.2.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.3.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.4.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.5.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.6.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.1.xS	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
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 またはそれ以降に移行して下さい。
3.2.xSE	脆弱性なし	脆弱性あり; 3.3.2SE に移行して下さい
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 またはそれ以降に移行して下さい。
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 またはそれ以降に移行して下さい。
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 またはそれ以降に移行して下さい。
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 またはそれ以降に移行して下さい。

3.5.xE	脆弱性なし	3.5.2E
3.6.xS	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
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 またはそれ以降に移行して下さい。
3.7.xE	脆弱性なし	脆弱性なし
3.8.xS	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。
3.9.xS	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。
3.10.xS	3.10.4S	3.10.4S
3.11.xS	脆弱性なし	脆弱性あり; 3.12S またはそれ以降に移行して下さい。
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 Cisco IOSソフトウェア Security Advisory によって組み込まれる書で表われる脆弱性の何れかから影響を受けません。

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 Cisco 内部テストの間に発見されました。

出典

URL

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

改訂履歴

リビジョン 1.0	2014-September-24	初回公開リリース

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。