Cisco IOSソフトウェア バーチャルルーティングおよび ICMP キュー ウェッジ脆弱性を転送すること

High

アドバイザリーID : cisco-sa-20150325-wedge

初公開日 : 2015-03-25 16:00

最終更新日 : 2016-01-14 17:27

バージョン 1.2 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCsi02145

CVE-2015-0638

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ソフトウェアのバーチャルルーティングおよびフォワーディング（VRF）サブシステム内の脆弱性はリモート攻撃者非認証によりサービス拒否（DoS）状態を引き起こすようにする可能性があります。

脆弱性はきちんと VRF 有効に された インターフェイスで受け取った悪意のある ICMP バージョン 4（ICMPv4）メッセージを処理する失敗が原因です。 攻撃者は設計されている ICMPv4 メッセージを入れることによって影響を受けたデバイスの脆弱性を引き起こすようにこの脆弱性を不正利用する可能性があります。 ICMPv4 メッセージが処理されるとき、影響を受けたインターフェイスのパケットキューはクリアされないかもしれウェッジをキューに導きます。 ウェッジが発生する場合、影響を受けたデバイスは Wedged Interface で受信された追加パケットを処理することを止めます。

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-20150325-wedge

注: 2015 年 3 月 25 日、Cisco IOS ソフトウェアおよび IOS XE ソフトウェアのセキュリティ アドバイザリにおいて、7 つの Cisco Security Advisory を含むバンドル資料を公開しました。 これ

らのアドバイザリは Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの脆弱性を扱っています。 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： Cisco IOS および IOS XE ソフトウェアに関するセキュリティ アドバイザリ公開資料*」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar15.html

該当製品

脆弱性のある製品

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 バージョンを実行している Ciscoデバイスは 1つ以上のインターフェイスが VRF インターフェイスに割り当てられるとき脆弱です。

デバイスのインターフェイスが VRF のために有効に なるかどうか判別するために、 **提示 VRF** コマンドラインインターフェイス exec CLI コマンドを使用して下さい。 デバイスが VRF のために設定されない場合、VRF が有効に なることを示す出力がありません。 次の例では、VRF はあらゆるインターフェイスで有効に なりません:

```
Router#show vrf
Router#
```

デバイスが VRF のために設定される場合、出力は VRF が次の例に示すように有効に なったデバイス インターフェイスを識別するために有効に なることを示したものです、:

```
Router#show vrf
Name Default RD Protocols Interfaces VRF-01 <not-set> ipv4 Gi0/0
```

先行する出力が戻るが、インターフェイスが割り当てられない場合、VRF は設定されるかもしれませんが、インターフェイスで有効に なりません。 この出力は次の例でこの場合示されています:

```
Router#show vrf
Name Default RD Protocols Interfaces VRF-01 <not-set> ipv4
```

デバイスへの IPv4 トラフィック 誘導だけ脆弱性を引き起こします。

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。 システム バナーに「Cisco Internetwork Operating System Software」や「Cisco IOS Software」などのテキストが表示された場合は、デバイスが Cisco IOS ソフトウェアを実行しています。 カッコ内にイメージ名が表示され、その後ろに Cisco IOS ソフトウェアのリリース番号とリリース名が続きます。 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), Version 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), Version 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

Cisco IOS XE ソフトウェアはこの脆弱性から影響を受けません。

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 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。

詳細

実行するデバイス Cisco IOS およびバーチャルルーティングを行うために設定されておよびフォワーディング（VRF）は VRF のために有効に なる インターフェイスに向かう ICMP バージョン 4 （ICMPv4）メッセージの処理の間に引き起こされるかもしれない脆弱性から影響を受けます。脆弱性はきちんと VRF 有効に された インターフェイスで受け取った悪意のある ICMPv4 メッセージを処理する失敗が原因です。 悪意のある ICMP メッセージは影響を受けたインターフェイスのパケットキューを入力するとき、きちんとまたはインプットキューからキュー ウェッジに終って、クリアされないそうではないかもしれません処理しないためにかもしれないし。 ウェッジが発生する場合、影響を受けたデバイスは Wedged Interface で受信された追加パケットを処理することを止めます。

キュー ウェッジはある特定のパケットが Cisco IOS ルータによってまたは切り替えたりキューから受信されか、が、キューに入るとき、プロセスエラーが原因で、決して取除かれません発生しません。 Cisco IOSソフトウェアのブロックされたインターフェイスを識別するのに使用するかもしれないいくつかの検知機構およびキュー ウェッジに関する詳細についてはこのアドバイザリの「回避策」セクションを参照して下さい。 また 説明される Ciscoセキュリティ ブログ Cisco IOS キュー ウェッジを参照して下さい。

IPバージョンのための ICMP はデバイスを通過する 4 つの（IPv4）メッセージこの脆弱性を引き起こしません; 影響を受けたデバイスで終端させるパケットだけ脆弱性を引き起こすことができます。

この脆弱性 Cisco バグ ID CSCsi02145 （ 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-2015-0638 は割り当てられました。

回避策

この脆弱性のための回避策がありませんが、次の識別 メカニズムはこの脆弱性のためにあります:

組み込みイベント マネージャ

脆弱 な Cisco IOSデバイスで Cisco IOS Embedded Event Manager（EEM） ポリシーが Tool Command Language （Tcl）に基づいているこの脆弱性によって引き起こされるインターフェイス キュー ウェッジを識別し、検出するのに使用することができます。 ポリシーはインターフェイス インプットキューが時管理者が Cisco IOSデバイスのためのインターフェイスを監視し、検出することを可能にします。 Cisco IOS EEM がこの脆弱性の潜在的な不正利用を検出するとき、ポリシーはアップグレードを設定することにする可能性があるか適した軽減を設定するか、またはインプットキューをクリアするためにデバイスをリロードするネットワーク管理者へアラートを送信 することによって応答を引き起こすことができます。

Tcl スクリプトは「Cisco で向こうダウンロード可能です: 次のリンクの組み込みイベント マネージャ（EEM）スクリプトを書くコミュニティ」: https://supportforums.cisco.com/docs/DOC-19337

説明される その他の情報に関しては、Ciscoセキュリティ ブログ Cisco IOS キュー ウェッジを参照して下さい。

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 Cisco Security Advisories, Responses, and Alerts 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、Cisco IOS ソフトウェアの脆弱性にさらされてい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（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入れたり、特定の資料のみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

このツールを使うことで、そのソフトウェア リリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（"First Fixed"）を特定できます。 また該当する場合、すべてのアドバイザリの脆弱性が修正された最初のリリース（"Combined First Fixed"）を特定できます。 Cisco IOS Software Checker を参照するか、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、いずれかの公開された Cisco IOS ソフトウェア アドバイザリに該当するかどうかを判断できます。

（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文書で表われる脆弱性から影響を受けません。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、2015 年 3 月の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドルに含まれている脆弱性の影響を受けません。

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。

この脆弱性は Cisco TAC によってユーザが抱える問題の調査の間に検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-wedge

改訂履歴

Vers	Description	Sect	Sta	日付

ion		ion	tus	
1.2	過去に公開されたすべてのCisco IOSソフトウェア セキュリティ アドバイザリを照会できる Cisco IOS Checker ソフトウェアの Checker フォームを更新しました。			2016 年 1 月 14 日
1.1	マイナーは脆弱なプロダクト セクションに影響を受け、ちょうど物理インターフェイスによってがある VRF に割り当てられる仮想インターフェイスさせるか、または物理的こと明白になるために編集します。			2015-March-26
1.0	初回公開リリース			2015 年 3 月 25 日

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。