Cisco IOSソフトウェアの多重 脆弱点はドメイン ネーム システム（DNS）マルチキャストしました

High	**アドバイザリーID :** cisco-sa-20140924-mdns **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 :** CSCul90866 CSCuj58950	CVE-2014-3357 CVE-2014-3358

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

マルチキャスト ドメイン ネーム システム（DNS）（mDNS）機能の Cisco IOSソフトウェア 実装は非認証を可能にする可能性があるサービス拒否（DoS）状態を引き起こすために mDNS パケットを処理するときリモート攻撃者次の脆弱性が含まれています:

- Cisco IOSソフトウェア mDNS ゲートウェイ メモリリーク の 脆弱性
- Cisco IOSソフトウェア mDNS ゲートウェイ サービス拒否の脆弱性

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。 このアドバイザリは、次のリンクより確認できます。
924-mdns

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。 すべてのアドバイザリは 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

影響を受けた Cisco IOSソフトウェアか Cisco IOS XE ソフトウェアを実行している Ciscoデバイスは脆弱です。 Cisco mDNS ゲートウェイ機能は有効に されたデフォルトで on Cisco IOS および Cisco IOS XE ソフトウェアです。 mDNS パケットを処理するのに必要とされる影響を受けたデバイスに特定の設定がありません。

Cisco IOSデバイスまたは Cisco IOS XE デバイスが mDNS パケットを処理し、デバイスにログイン し、次の Command Line Interface（ CLI ）コマンドの発行するかどうか判別することは **IP ソケットを、 show udp 示すか**、または **コントロール・プレーン ホスト 開港を示します。** 出力がポート UDP 5353 で受信する IP アドレスを示したもので場合デバイスは脆弱です。

次の例はこれらの脆弱性から影響を受ける Cisco IOSデバイスを示したものです。 デバイスはソケットが UDP ポート 5353 で開くので脆弱です:

```
Router#show ip socket
Proto Remote Port Local Port In Out Stat TTY OutputIF
17 --listen-- 192.168.0.1 67 0 0 1 0
17 --listen-- 192.168.0.1 68 0 0 1 0
17 --listen-- 224.0.0.251 5353 0 0 1 0
Router#

Router#sho udp
Proto        Remote      Port      Local       Port  In Out  Stat TTY OutputIF
17     224.0.0.251      5353 --any--          5353   0   0 1000021   0
17(v6) FF02::FB         5353 --any--          5353   0   0 1020021   0
Router#

Router#sho control-plane host open-ports
Active internet connections (servers and established)
Prot               Local Address            Foreign Address                  Service    State
 tcp                       *:22                       *:0                  SSH-Server   LISTEN
 tcp                       *:23                       *:0                      Telnet   LISTEN
 udp                     *:5353             224.0.0.251:0          IOS host service   LISTEN
Router#
```

注: Cisco バグ ID CSCum51028 のための修正前の Cisco IOS および Cisco IOS XE ソフトウェアの動作はデフォルトで mDNS 機能をつけることです。 この動作は Cisco バグ ID CSCum51028 によって変更され、今デフォルトでディセーブルにされます。 管理者が mDNS 機能を有効に したいと思う場合デバイスで手動で設定する必要があります。

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。 "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

Cisco IOS XR ソフトウェアは、これらの脆弱性の影響を受けません。

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

サブネットを渡るサービスおよびデバイスに制御されたおよび安全なアクセスを可能にする Cisco のサービス検出ゲートウェイ（mDNS ゲートウェイ）は IOS コンポーネントです。 それはすべての構成されたネットワーク セグメントの発表を保守するために受信し、サービスおよびアドレスのキャッシュを構築します。

Cisco IOSソフトウェア mDNS ゲートウェイ メモリリーク の 脆弱性

Cisco IOSソフトウェアのマルチキャスト ドメイン ネーム システム（DNS）（mDNS）実装の脆弱性は非認証により、リモート攻撃者影響を受けたデバイスのインターフェイス ウェッジかリロードに結局導く可能性があるメモリリーク状態を引き起こすようにする可能性があります。

脆弱性は影響を受けたデバイスに送信される不正 な mDNS パケットの不適当な解析が原因です。 攻撃者は影響を受けたデバイスが処理される不正 な mDNS パケットの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により影響を受けたデバイスのインターフェイス ウェッジかリロードに結局導く可能性があるメモリリーク状態を引き起こすことを可能にする可能性があります。

この脆弱性は IPv4 および IPv6 両方パケットを使用して不正利用することができます。 脆弱性はデバイス、IPv4 マルチキャスト アドレス 224.0.0.251、または IPv6 マルチキャスト アドレス FF02::FB で設定されるあらゆるインターフェイスの IPv4/IPv6 ユニキャスト アドレスを使用してポート 5353 に宛てた不正 な UDP パケットによって引き起こすことができます。

この脆弱性は影響を受けたデバイスに向かうトラフィックによってしか引き起こし、影響を受けたデバイスを通過するトラフィックと不正利用することができません。

脆弱 な 設定の基準を満たすデバイスでは、不正 な UDP mDNS パケットはこの脆弱性を引き起こす可能性があります。 インフラストラクチャのナレッジの攻撃者はこの脆弱性を不正利用するために設定された 条件の mDNS パケットを細工 する可能性があります。 脆弱性の不正利用の成功は影響を受けたデバイスのインターフェイス ウェッジおよび結局リロードに導く場合があるメモリリークという結果に終る可能性があります。 インターフェイスキュー ウェッジ状態からのリカバリはサービス拒否 （ DoS ）状態という結果に終る可能性があるデバイスのリロードを必要とします。

インターフェイスキュー 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、キューに入るプロセスエラーによる脆弱性のクラス決して取除かれませんではないです。 ブロックされたインターフェイス IOS software を on Cisco 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 Ciscoセキュリティ ブログ「Cisco IOS キュー」が次のリンクで説明されて詰め込むことを参照して下さい: http://blogs.cisco.com/security/cisco_ios_queue_wedges_explained/

この脆弱性 Cisco バグ ID CSCuj58950 （ 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-2014-3358 は割り当てられました。

Cisco IOSソフトウェア mDNS ゲートウェイ サービス拒否の脆弱性

Cisco IOSソフトウェアのマルチキャスト DNS （ mDNS ）ゲートウェイ機能の脆弱性はリモート攻撃者非認証が脆弱 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。

脆弱性は mDNS パケットの不適当な検証が原因です。 攻撃者は UDP ポート 5353 の不正 な IPv4 または IPv6 パケットの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者によりサービス拒否 （ 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。

この脆弱性は IPv4 および IPv6 両方パケットを使用して不正利用することができます。 脆弱性はデバイス、IPv4 マルチキャスト アドレス 224.0.0.251、または IPv6 マルチキャスト アドレス FF02::FB で設定されるあらゆるインターフェイスの IPv4/IPv6 ユニキャスト アドレスを使用してポート 5353 に宛てた不正 な UDP パケットによって引き起こすことができます。

この脆弱性は影響を受けたデバイスに向かうトラフィックによってしか引き起こし、影響を受けたデバイスを通過するトラフィックと不正利用することができません。

脆弱 な 設定の基準を満たすデバイスでは、不正 な UDP mDNS パケットはこの脆弱性を引き起こす可能性があります。 インフラストラクチャのナレッジの攻撃者はこの脆弱性を不正利用する

ために設定された 条件の mDNS パケットを細工 する可能性があります。 脆弱性の不正利用の成功は影響を受けたデバイスのリロードという結果に終る場合があります。

この脆弱性は Cisco バグ ID CSCul90866 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3357 を割り当てられました。

セキュリティ侵害の痕跡

回避策

アクセス コントロール リスト

on Cisco Cisco バグ ID CSCum51028 のための修正がない IOS および Cisco IOS XE ソフトウェア リリースに、そこに現在 手動で ポートを閉じるか、またはサービスをディセーブルにする方法ではないです。

それらのリリースで、可能性のある回避策は UDP ポート 5353 に向かうトラフィックをブロックするためにインターフェイスに作成され、適用することができる拡張 Access Control List （ACL）の設定で構成されています。

この脆弱性の mDNS 機能は転送するとして UDP を利用するので、信頼された IP アドレスからのこれらのポートに ACL をその割り当て通信敗北させるかもしれない送信側の IP アドレスをスプーフィングすることは可能性のあるです。 ACL に加えて、管理者は転送されるパケットの送信元アドレスの到達可能性を確認する Cisco IOSソフトウェアのセキュリティ機能 uRPF を有効にする必要があります。 これら二つのテクノロジーの組み合せは単独で ACL より強い回避策を提供します。

ACL 下記の例は UDP ポート 5353 に向かうトラフィックからデバイスの保護を助ける展開されたインターフェイス access-list の一部として含まれるはずです:

```
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
```

コントロール プレーン ポリシング

コントロール プレーン ポリシング（CoPP）がデバイスに信頼できない UDP トラフィックをブロックするのに使用することができます。 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 はデバイスで管理および制御平面を保護し、既存 の セキュリティポリシーおよびコンフィギュレーションに従ってインフラストラクチャ デバイスに送信 される 明示的に承認されたトラフィックだけ許可することによって直接インフラストラクチャ不正侵入のリスクおよび効果を最小に するのを助けるために設定することができます。

CoPP 下記の例は UDP ポート 5353 に向かうトラフィックからデバイスの保護を助ける展開された CoPP の一部として含まれるはずです:

```
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 上の例では、「拒否」操作を一致するパケットは policy-map 「ドロップする」機能から（示されていない）影響を受けないが policy-map 「ドロップする」機能によって廃棄されるこれらのパケットの「割り当て」アクションの結果を用いる潜在的なエクスプロイト パケット一致する アクセス制御リスト エントリ（ACE）その。 以下の事項に注意して下さい: policy-map 構文は 12.2S および 12.0S 一連のCisco IOSソフトウェアで異なっています:

```
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
```

注: Cisco は IPv6 トラフィックのための CoPP を展開することを推奨しません。

CoPP 機能の設定および使用のその他の情報は文書で「コントロール プレーン ポリシング 実装 最良 の 方法」および次のリンクの「コントロール プレーン ポリシング」見つけることができます: 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

on Cisco Cisco バグ ID CSCum51028 のための修正がある IOS および Cisco IOS XE ソフトウェア リリースにサービス **ルーティング mdns sd** コマンドラインインターフェイス グローバルコンフィギュレーション（CLI）コマンドの設定なによって、mDNS ゲートウェイ機能ディセーブルにすることができます。

次の識別 メカニズムは Cisco IOSソフトウェア mDNS メモリリーク 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 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

また Ciscoセキュリティ ブログ「Cisco IOS キュー」が次のリンクで説明されて詰め込むことを参照して下さい: http://blogs.cisco.com/security/cisco_ios_queue_wedges_explained/

ネットワーク内のシスコ デバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Mitigation Bulletin』を参照してください。以下のリンクから入手できます。 http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=35023

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アドバイザリ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、またはすべてのアドバイザリ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

ツールは各 Cisco Security Advisory のすべての脆弱性を解決する以前のリリースおよび問い合わせられたソフトウェア 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、ツールはまた最も早い可能性のある リリースを戻しますすべての表示する アドバイザリのすべての脆弱性を解決する（「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アドバイザリ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、この資料で情報開示された脆弱性の影響を受けます。

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 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 Cisco IOSソフトウェア Security Advisory によって組み込まれる書のすべてのアドバイザリ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 またはそれ以降への移行する。
2.2.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降への移行する。
2.3.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降への移行する。
2.4.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降への移行する。
2.5.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降への移行する。
2.6.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降への移行する。
3.1.xS	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降への移行する。
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 またはそれ以降への移行する。
3.2.xSE	脆弱性なし	脆弱性あり; 3.3.2SE への移行する
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 またはそれ以降への移行する。
3.3.xSE	3.3.2SE	3.3.2SE
3.3.x	脆弱。	脆弱性あり; 3.4.4SG またはそれ

SG		以降への移行する。
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 またはそれ以降への移行する。
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 またはそれ以降への移行する。
3.5.xE	3.5.2E	3.5.2E
3.6.xS	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降への移行する。
3.6.xE	脆弱性なし	脆弱性なし
3.7.xS	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降への移行する。
3.7.xE	脆弱性なし	脆弱性なし
3.8.xS	脆弱性なし	脆弱性あり; 3.10.4S またはそれ以降への移行する。
3.9.xS	脆弱性なし	脆弱性あり; 3.10.4S またはそれ以降への移行する。
3.10.xS	脆弱性なし	3.10.4S
3.11.xS	3.11.1S	脆弱性あり; 3.12S またはそれ以降への移行する。
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 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

る脆弱性の不正利用事例とその公表は確認しておりません。

これらの脆弱性は内部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-20140924-mdns

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。