Cisco IOS Software DHCP Denial of Service Vulnerability

Advisory ID: cisco-sa-20120926-dhcp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp

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 2012 September 26 16:00 UTC (GMT)

内容

要約

Cisco IOS ソフトウェアには、認証されていないリモートの攻撃者がサービス拒否（DoS）状態を引き起こす可能性のある脆弱性が存在します。攻撃者は、1 つの DHCP パケットを該当デバイスに送信または通過させることで、この脆弱性を不正利用できる可能性があります。その結果、デバイスでは再起動が発生します。

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、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp

注：2012 年 9 月 26 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 9 件の Cisco Security Advisory が含まれています。8 件のアドバイザリは Cisco IOS ソフトウェアの脆弱性に対処するもので、1 件は Cisco Unified Communications Manager の脆弱性に対処するものです。各 Cisco IOS ソフトウェア セキュリティ アドバイザリには、そのアドバイザリで詳述された脆弱性を解決する Cisco IOS ソフトウェア リリース、および 2012 年 9 月にバンドル公開したすべての Cisco IOS ソフトウェアの脆弱性を解決する Cisco IOS ソフトウェア リリース

を記載しています。

個々の公開リンクは、次のリンクにある「Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication」内に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html

該当製品

脆弱性が存在する製品

Device Sensor 機能を含む Cisco IOS ソフトウェア バージョンが実行されているシスコ デバイスは、この脆弱性の影響を受けます。IP アドレスとのインターフェイスが少なくとも 1 つあるデバイスが該当します。

Cisco IOS ソフトウェア リリースに Device Sensor 機能が含まれているかどうかを確認するには、 **show subsys** コマンドを実行します。

次の例では、Device Sensor 機能が含まれています。

```
Switch#show subsys | include dsensor_lite
dsensor_lite                          Protocol     1.000.001
```

インターフェイスに IP アドレスが割り当てられているかどうかを確認するには、 **show ip interface brief** コマンドを実行します。

次の例では、FastEthernet1/0 インターフェイスに IP アドレス 10.10.10.1 が割り当てられています。

```
router#show ip interface brief   Interface              IP-Address      OK? Method Status
        Protocol  FastEthernet1/0          10.10.10.1      YES manual up                    up
    FastEthernet1/1          unassigned      YES NVRAM  up                    up
```

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 15.0(1)M1 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), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_teamRouter> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
```

Cisco IOS ソフトウェアのリリース命名規則の追加情報は以下のリンクにある「White Paper: Cisco IOS and NX-OS Software Reference Guide」で確認できます。
http://www.cisco.com/web/about/security/intelligence/ios-ref.html

脆弱性が存在しない製品

Cisco IOS XE ソフトウェアおよび Cisco IOS XR ソフトウェアは、こ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 ソフトウェアの Device Sensor 機能は、Cisco Discovery Protocol、Link Layer Discovery Protocol（LLDP）、DHCP などのプロトコルを使用するネットワーク デバイスからエンドポイントの Raw データを収集するときに使用します。エンドポイント データは、登録されたクライアントがアクセス セッションから利用できます。

Cisco IOS ソフトウェアには、認証されていないリモートの攻撃者が DoS 状態を発生させる可能性のある脆弱性が含まれています。攻撃者は、1 つの DHCP パケットを該当デバイスに送信または通過させることで、この脆弱性を不正利用できる可能性があります。その結果、デバイスでは再起動が発生します。

デフォルトで有効な Device Sensor 機能は、IP アドレスが割り当てられたインターフェイスを少なくとも 1 つ持つデバイスにおいて脆弱となります。この脆弱性は、Device Sensor 機能が DHCP パケットを処理しようとしたときに発生します。該当のリリースでは、有効な DHCP パケットがこの脆弱性を引き起こす可能性があります。

Device Sensor 機能の詳細については、『Device Sensor Guide』を参照してください。

この脆弱性は、すでに Cisco Bug ID CSCty96049（登録ユーザのみ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2012-4621 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ 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導き出すことができます。

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、シスコは個々の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/

CSCty96049 - Cisco IOS Software DHCP Server Denial of Service 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

この脆弱性が悪用されると、 該当するデバイスが再起動する可能性があります。また、繰り返し悪用されると、継続的な DoS 状態とな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 and Responses アーカイブや、本アドバイザリ以降に公開のアドバイザリを参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が不明確な場合は、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 IOS ソフトウェア テーブル（下記）の各行は Cisco IOS ソフトウェア トレインを示します。あるトレインが脆弱性を含む場合、修正を含む最初のリリースは「First Fixed Release」列に示されます。「First Fixed Release for All Advisories in the September 2012 Bundled Publication」列は、その Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開で公

開済みであるすべての脆弱性を修正する最初のリリースを示します。シスコは利用可能な最新のリリースへのアップグレードを推奨します。

Cisco IOS ソフトウェア チェッカーを利用して、特定の Cisco IOS ソフトウェア リリースに対応したシスコのセキュリティ アドバイザリを検索することができます。このツールは次の Cisco Security Intelligence Operations（SIO）ポータルで利用できます。
http://tools.cisco.com/security/center/selectIOSVersion.x

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Secur Advisory Bundled Publication
There are no affected 12.0 based releases		
Affected 12.2-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Secur Advisory Bundled Publication
There are no affected 12.2 based releases		
Affected 12.3-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Secur Advisory Bundled Publication
There are no affected 12.3 based releases		
Affected 12.4-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Secur Advisory Bundled Publication
There are no affected 12.4 based releases		
Affected 15.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Secur Advisory Bundled Publication
15.0EX	Not vulnerable	Not vulnerable
15.0EY	Not vulnerable	Not vulnerable
15.0M	Not vulnerable	15.0(1)M9
15.0MR	Not vulnerable	Vulnerable; contact your support organizati the instructions in Obtaining Fixed Software section of this advisory.
15.0MRA	Not vulnerable	Vulnerable; contact your support organizati the instructions in Obtaining Fixed Software section of this advisory.
15.0S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(1)S6 Cisco IOS XE devices: Please see Cisco IO Software Availability
15.0SE	15.0(1)SE3 15.0(2)SE 15.0(2)SE1; Available on 10-DEC-12	15.0(2)SE
15.0SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(2)SG5 15.0(2)SG6 ; Available on 11-OCT-12 Cisco IOS XE devices: Please see Cisco IO Software Availability
15.0SY	Not vulnerable	15.0(1)SY2
15.0XA	Not vulnerable	Vulnerable; First fixed in Release 15.1M
15.0XO	Cisco IOS XE devices: Please see Cisco IOS-	

	XE Software Availability	Cisco IOS XE devices: Please see Cisco IO Software Availability
Affected 15.1-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Secur Advisory Bundled Publication**
15.1EY	Not vulnerable	15.1(2)EY4
15.1GC	Not vulnerable	Vulnerable; First fixed in Release 15.1M
15.1M	Not vulnerable	15.1(4)M5
15.1MR	Not vulnerable	15.1(3)MR; Available on 01-OCT-12
15.1S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(3)S Cisco IOS XE devices: Please see Cisco IO Software Availability
15.1SG	15.1(1)SG1 15.1(2)SG; Available on 12-NOV-12 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(1)SG1 15.1(2)SG 12-NOV-12 Cisco IOS XE devices: Please see Cisco IO Software Availability
15.1SNG	Not vulnerable	Vulnerable; contact your support organizati the instructions in Obtaining Fixed Software section of this advisory.
15.1SNH	Not vulnerable	Vulnerable; contact your support organizati the instructions in Obtaining Fixed Software section of this advisory.
15.1SNI	Not vulnerable	Vulnerable; migrate to any release in 15.2S
15.1SV	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organizati the instructions in Obtaining Fixed Software section of this advisory.
15.1T	Not vulnerable	Vulnerable; First fixed in Release 15.1M
15.1XB	Not vulnerable	Vulnerable; First fixed in Release 15.1M
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Secur Advisory Bundled Publication**
15.2GC	Not vulnerable	Releases prior to 15.2(3)GC are vulnerable Releases 15.2(3)GC and later are not vulnerable.First fixed in Release 15.2T
15.2JA	Not vulnerable	Not Vulnerable
15.2M	Not vulnerable	Not vulnerable
15.2S	15.2(2)S1 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.2(1)S2 15.2(2)S1 15.2(4)S Cisco IOS XE devices: Please see Cisco IO Software Availability
15.2SNG	Not vulnerable	Not vulnerable
15.2T	Not vulnerable	15.2(1)T3 15.2(2)T2 15.2(3)T2; Available on 12-OCT-12

Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェアは、この脆弱性の影響を受けません。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、この脆弱性の影響を受けません。

回避策

該当するリリースでは、Device Sensor 機能はデフォルトで有効になっています。このアドバイザリに示されている脆弱性は、グローバル コンフィギュレーション コマンド **device-sensor filter-spec dhcp exclude all** を適用することで緩和できます。このコマンドは、Device Sensor 機能による DHCP パケット収集をフィルタリングするため、Device Sensor 機能で DHCP 情報を処理または保存することがなくなります。

次の例では、グローバル コマンドを実行しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
```

Device Sensor 機能で DHCP データが収集されなくなったかどうかを確認するには、 **show device-sensor cache all** コマンドを実行します。テーブルに DHCP エントリが表示されていなければ収集されていません。

次の例では、テーブル内に Cisco Discover Protocol データのみが含まれています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
```

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に特有の問題に関してご確認ください。

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、適切な処置について支援を受けてください。

回避策の効果は、使用製品、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のお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とする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か、お客様のサービス プロバイダーやサポート会社にご相談ください。

サービス契約をご利用でないお客様

シスコから直接購入したが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、サードパーティ ベンダーから購入したが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を入手してください。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このアドバイザリの 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 を通して無償アップグレードをお求めください。

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を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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、お客様からのお問い合わせへの対応の際に発見されました。

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。またシスコシステムズ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-20120926-dhcp

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

このアドバイザリに関する今後の更新があれば、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。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.0	2012-September-26	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支援、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について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。この Web ページには、シスコのセキュリティ アドバイザリ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。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。