Cisco適応型セキュリティアプライアンスソフトウェアのDHCPv6リレーにおけるDoS脆弱性

High

アドバイザリーID : cisco-sa-20160420-asa-dhcpv6

初公開日 : 2016-04-20 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 : CSCus23248

CVE-2016-1367

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適応型セキュリティアプライアンス(ASA)ソフトウェアのDHCPv6リレー機能の脆弱性により、認証されていないリモートの攻撃者が該当デバイスのリロードを引き起こす可能性があります。

この脆弱性は、DHCPv6パケットの不十分な検証に起因します。攻撃者は、巧妙に細工されたDHCPv6パケットを該当デバイスに送信することで、この脆弱性を不正利用し、サービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、シングルコンテキストモードまたはマルチコンテキストモードで、ルーテッドファイアウォールモードに設定されたシステムに影響します。Cisco ASAソフトウェアがこの脆弱性の影響を受けるのは、ソフトウェアにDHCPv6リレー機能が設定されている場合だけです。この脆弱性は、IPv6トラフィックによってのみ引き起こされます。

この脆弱性の影響を受けるのは、Cisco ASAソフトウェアリリース9.4.1だけです。

シスコはこ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。この脆弱性に対処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で確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-asa-dhcpv6

該当製品

次の製品で実行されているCisco ASAソフトウェアは、この脆弱性の影響を受ける可能性があります。

- Cisco ASA 5500-X シリーズ次世代ファイアウォール
- Cisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用Cisco ASAサービスモジュール
- Cisco 適応型セキュリティ仮想アプライアンス（ASAv）

影響を受けるリリースの詳細については、このセキュリティアドバイザリの「修正済みソフトウェア」セクションを参照してください。

脆弱性のある製品

Cisco ASAソフトウェアは、DHCPv6リレー機能が設定されている場合にのみ、この脆弱性の影響を受けます。DHCPv6リレー機能が設定されているかどうかを確認するには、 **show running-config ipv6 dhcprelay**コマンドを使用して、少なくとも1つのインターフェイスでその機能が有効になっていることを確認します。

次の例は、インターフェイス *outside*で有効になっているDHCPv6リレー機能を示しています。

```
asa#show running-config ipv6 dhcprelay
ipv6 dhcprelay enable outside
```

注：DHCPv6リレー機能はデフォルトでは設定されていません。

脆弱性を含んでいないことが確認された製品

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。

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

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リリースしています。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、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。お客様は、こ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することにより、シスコソフトウェアライセンスの条項に従うことに同意するものとします。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシ

スコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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 アーカイブや後続のアドバイザリを参照して、侵害を受ける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は新規リリースでも継続して適切なサポートが受けられることを確認してください。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。

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。
http://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

次の表に示すように、適切なリリースにアップグレードする必要があります。

表の左の列に、Cisco ASAソフトウェアのメジャーリリースを示します。右の列は、メジャー リリースが本アドバイザリに記載している脆弱性に該当するかどうか、また、本脆弱性に対する修正を含む最初のリリースに該当するかどうかを示します。

Cisco ASA メジャー リリース	First Fixed Release（修正された最初のリリース）
7.2	Not affected
8.0	Not affected
8.1	Not affected
8.2	Not affected
8.3	Not affected
8.4	Not affected
8.5	Not affected

8.6	Not affected
8.7	Not affected
9.0	Not affected
9.1	Not affected
9.2	Not affected
9.3	Not affected
9.4	9.4 (1.1)
9.5	Not affected
9.6	Not affected

ソフトウェアのダウンロード

Cisco ASAソフトウェアは、Cisco.comのSoftware Centerから http://www.cisco.com/cisco/software/navigator.htmlにアクセスしてダウンロードできます。

Cisco ASA 5500シリーズ適応型セキュリティアプライアンスおよびCisco ASA 5500-Xシリーズ次世代ファイアウォールの場合は、次のパスに移動します。暫定バージョンを検索するには、ダウンロードページの左側にある[All Releases] > [Interim] をクリックします。
[製品(Products)] > [セキュリティ(Security)] > [ファイアウォール(Firewalls)] > [適応型セキュリティアプライアンス(ASA)(Adaptive Security Appliances (ASA))] > [ASA 5500-Xシリーズファイアウォール(ASA 5500-X Series Firewalls)] > <Cisco ASAモデル> > [シャーシ上のソフトウェア(Software on Chassis)] > [適応型セキュリティアプライアンス(ASA)ソフトウェア(Adaptive Security Appliance (ASA) Software) Cisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用Cisco ASAサービスモジュールの場合は、次のパスに移動します。暫定バージョンを検索するには、ダウンロードページの左側にある[All Releases] > [Interim] をクリックします。
[製品(Products)] > [Cisco Interfaces and Modules] > [Services Modules] > [Catalyst 6500 Series / 7600 Series ASA Services Module] > [Adaptive Security Appliance(ASA)Software] Cisco適応型セキュリティ仮想アプライアンス(ASAv)の場合は、次のパスに移動します。
[製品(Products)] > [セキュリティ(Security)] > [ファイアウォール(Firewalls)] > [適応型セキュリティアプライアンス(ASA)(Adaptive Security Appliances (ASA))] > [適応型セキュリティアプライアンス(ASA)(Adaptive Security Appliance (ASA) Software)]

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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やその公表を確認していません。

出典

この脆弱性は、サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-asa-dhcpv6

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	-	Final	2016年4月20日

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。