Cisco ASAソフトウェアのDNSにおけるDoS脆弱性

High

アドバイザリーID : cisco-sa-20170419-asa-dns

初公開日 : 2017-04-19 16:00

バージョン 1.0 : Final

CVSSスコア : 8.1

回避策 : No workarounds available

Cisco バグ ID : CSCvb40898

CVE-2017-6607

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 ASAソフトウェアのDNSコードの脆弱性により、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したり、デバイスのローカルDNSキャッシュにある情報を破損させたりする可能性があります。

この脆弱性は、巧妙に細工されたDNS応答メッセージの処理に欠陥があることに起因します。攻撃者は、Cisco ASAソフトウェアからのDNS要求をトリガーし、巧妙に細工された応答で応答することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、デバイスがリロードされ、サービス拒否(DoS)状態またはローカルDNSキャッシュ情報の破損が発生する可能性があります。

注：この脆弱性の不正利用に使用できるのは、該当デバイス宛てのトラフィックだけです。この脆弱性は、ルーテッドファイアウォールモードまたはトランスペアレントファイアウォールモード、および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設定されたCisco ASAソフトウェアに影響を与えます。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされる可能性があります。

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、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-dns

該当製品

脆弱性のある製品

この脆弱性は、次の製品で実行されているCisco ASAソフトウェアに影響を与えます。

- Cisco ASA 1000V クラウド ファイアウォール
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- 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）
- Cisco Firepower 9300 ASAセキュリティモジュール
- Cisco ISA 3000 Industrial Security Appliance

該当す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。

Cisco ASAソフトウェアは、DNSサーバグループに少なくとも1つのDNSサーバIPアドレスが設定されている場合、この脆弱性の影響を受けます。これは、デフォルトのDNSサーバグループ(*DefaultDNS*)またはユーザ定義のDNSサーバグループの一部として設定できます。

DNSサーバのIPアドレスが設定されているかどうかを確認するには、 **show running-config dns server-group**コマンドを使用して、 **name-server**パラメータにIPアドレスが含まれていることを確認します。

次の例は、DNSサーバIP 192.168.1.1が *DefaultDNS*サーバグループの一部として設定されているCisco ASAソフトウェアアプライアンスを示しています。

```
ciscoasa# show running-config dns server-group
DNS server-group DefaultDNS     name-server 192.168.1.1 . . .
```

注：デフォルトでは、DNS name-server値はどのDNSサーバグループにも設定されていません。

実行中のソフトウェアリリースの確認

管理者は、Cisco ASA ソフトウェアの脆弱性が存在するリリースがアプライアンスで実行されているかどうかを確認するために **show version コマンドを使用できます。**次の例は、Cisco ASAソフトウェアリリース9.2(1)を実行しているアプライアンスでの結果を示しています。

```
ciscoasa# show version | include Version
Cisco Adaptive Security Appliance Software Version 9.2(1)
Device Manager Version 7.4(1)
```

Cisco Adaptive Security Device Manager（ASDM）を使用してデバイスを管理している場合は、ログイン ウィンドウ、または Cisco ASDM ウィンドウの左上にソフトウェア リリースが表示されます。

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。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、お客様は以下のリンクに記載された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。
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際には、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] ページで入手できるシスコ製品のアドバイザリを定期的に参照して、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。

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 Cisco Service Contract 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 POS から入手できない場合は、Cisco 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。

修正済みリリース

次の表では、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 ソフトウェア メジャー リリース	First Fixed Release（修正された最初のリリース）
9.01	影響あり、9.1(7.12)以降に移行
9.0[1]	影響あり、9.1(7.12)以降に移行
9.1	9.1(7.12) 以降
9.2	9.2(4.18) 以降
9.31	影響あり、9.4(3.12)以降に移行
9.4	9.4(3.12) 以降
9.5	9.5(3.2) 以降
9.6	9.6(2.2) 以降
9.7	Not affected
9.8	Not affected

[1] Cisco ASAソフトウェアリリース9.1より前のリリースとCisco ASAソフトウェアリリース9.3は、ソフトウェアメンテナンスが終了しています。お客様は、サポートされているリリースに移行する必要があります。

注：この脆弱性に対する特定の修正済みソフトウェアリリースは、 Cisco Field Notice FN-64291に記載されている不具合の影響を受ける可能性があります。この不具合では、213日の稼動後にセキュリティアプライアンスがトラフィックの受け渡しに失敗する可能性があります。お客様は、このアドバイザリに記載されている脆弱性に対処する方法を決定する前に、このField Noticeを確認する必要があります。Cisco Field Noticeで説明されている問題は、セキュリティの脆弱性ではありません。

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

この脆弱性は内部テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-dns

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	2017 年 4 月 19 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。