

Cisco IOS および IOS XE ソフトウェア DNS フォワーダ サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20160928-dns

[CVE-2016-6380](#)

初公開日 : 2016-09-28 16:00

バージョン 1.0 : Final

CVSSスコア : [8.3](#)

回避策 : [Yes](#)

Cisco バグ ID : [CSCup90532](#)

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 および IOS XE ソフトウェアの DNS フォワーダ 機能の脆弱性はリロードするか、デバイスのローカル DNS キャッシュで現在の情報を破損するかまたはプロセス メモリの一部を読みます非認証、リモート攻撃者によりデバイスはことを可能にする可能性があります。

脆弱性は処理によって細工される DNS 応答メッセージの欠陥が原因です。攻撃者は影響を受けたデバイスから DNSサーバへの転送されたクライアント DNS クエリに DNS 応答メッセージを代行受信することおよび細工することによってこの脆弱性を不正利用する可能性があります。正常なエクスプロイトによりデバイスはローカル DNS キャッシュ情報のサービス拒否 (DoS) 条件が破損に終って、リロードしやす可能性があります。

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。この脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-dns>

このアドバイザリーは、2016年9月28日に公開された11件の脆弱性に関する10件のシスコセキュリティアドバイザリーを含むCisco IOS ソフトウェアおよびIOS XE ソフトウェア リリースのセキュリティアドバイザリーバンドルの一部です。このすべての脆弱性はセキュリティへの影響が「高」と評価されています。それらへのアドバイザリーおよびリンクの完全なリストに関しては、[Cisco イベント応答が表示されて下さい : 9月 2016 年半年ごと Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書。](#)

該当製品

修正済みソフトウェア

この脆弱性は Cisco IOSソフトウェアまたは Cisco IOS XE ソフトウェアの脆弱なリリースを実行する製品に影響を及ぼします。Cisco IOS および IOS XE ソフトウェア リリースが脆弱である情報に関しては、このアドバイザリの[修正済みソフトウェアのセクション](#)を参照して下さい。

実行するデバイスはコードの脆弱なリリース IP DNSサーバ 機能が有効になる場合影響を受けています。DNSサーバ 機能はデフォルトで有効になりません。

デバイスが DNSサーバ 機能のために設定されるかどうか確かめるために、**show running-config** を使用して下さい | **ip dns server** コマンドを含み、機能があることを確認して下さい。次の例は有効になる DNSサーバ 機能を用いる Cisco IOS ルータを示したものです:

```
router#show running-config | include ip dns server
ip dns server
```

Cisco IOS ソフトウェア リリースの判別

、管理者はデバイスにログインどの Cisco IOS ソフトウェア リリースがデバイスで動作しているか判別し、**show version** コマンドを Command Line Interface (CLI) で使用し、次に現われるシステムバナーを参照するためにできます。デバイスが Cisco IOSソフトウェアを実行する場合、システムバナーは *Cisco Internetwork Operating System software* か *Cisco IOS*ソフトウェアと同じようなテキストを表示する。バナーにはインストールされたイメージ名もカッコ内に表示されます。その後ろには Cisco IOS ソフトウェアのリリース番号とリリース名も表示されます。いくつかの Cisco デバイスは **show version** コマンドをサポートしませんし、別の出力を提供しないかもしれません。

次の例は、Cisco IOS ソフトウェア リリースが 15.5(2)T1、インストールされたイメージ名が C2951-UNIVERSALK9-M であるシスコ製品を示しています。

```
Router> show version
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
.
```

Cisco IOS ソフトウェア リリースのための指名および番号付与規則についての情報に関しては、[白書を参照して下さい: Cisco IOS および NX-OS ソフトウェア レファレンスガイド](#)。

Cisco IOS XE ソフトウェア リリースの判別

、管理者はデバイスにログインどの Cisco IOS XE ソフトウェア リリースがデバイスで動作しているか判別し、**show version** コマンドを CLI で使用し、次に現われるシステムバナーを参照

するためにできます。デバイスが Cisco IOS XE ソフトウェアを実行する場合、システムバナーは *Cisco IOS XE* ソフトウェアが同じようなテキストを表示する。

次の例は Cisco IOS XE ソフトウェア リリース 3.16.1aS を実行しているデバイスの **show version** コマンドの出力を示したものです：

```
Router> show version
Cisco IOS XE Software, Version 03.16.01a.S - Extended Support Release
Cisco IOS Software, ASR1000 Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.5(3)S1a,
RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Nov-15 17:40 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェア リリースのための指名および番号付与規則についての情報に関しては、[白書を参照して下さい](#)：[Cisco IOS および NX-OS ソフトウェア レファレンスガイド](#)。

脆弱性を含んでいないことが確認された製品

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。

シスコは、この脆弱性が Cisco IOS XR ソフトウェアまたは Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

改訂履歴

| Version | Description | Section | Status | 日付 |
|---------|-------------------------|---------|--------|-----------------|
| 1.0 | Initial public release. | | Final | 2016 年 9 月 28 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、単独の転載や意識を施した場合、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。