

Cisco IOSソフトウェア ネットワーク アドレス 変換 (NAT) 脆弱性

High	アドバイザーID : cisco-sa-20100922-nat	CVE-2010-2833
	初公開日 : 2010-09-22 16:00	CVE-2010-2832
	最終更新日 : 2012-09-21 19:14	CVE-2010-2831
	バージョン 1.1 : Final	
	CVSSスコア : 7.8	
	回避策 : Yes	
	Cisco バグ ID : CSCtd86472 , CSCtf17624 , CSCtf91428	

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® ソフトウェア ネットワーク アドレス変換 (NAT) 機能は 3 サービス拒否 (DoS) 脆弱性が含まれています。最初の脆弱性はセッション開始プロトコル (SIP) パケットの変換に、H.323 パケットの変換の 2つめの脆弱性あり、第 3 脆弱性は H.323 パケットのための H.225.0 呼出し シグナリングの変換にあります。

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。

このアドバイザーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-nat> で掲示されます。

注: 2010 年 9月 22 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。アドバイザーの 5 つは Cisco IOSソフトウェアの脆弱性に対処し、1 つのアドバイザーは Cisco Unified Communications Manager の脆弱性に対処します。各アドバイザーには、そのアドバイザーで詳述された脆弱性を解決するリリースを記載しています。次の URL リストの表は正しい 2010 年 9月 22 日送達されたすべての Cisco IOSソフトウェア脆弱性、またはそれ以前ことリリースします:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-bundle>

"Cisco Event Response: 半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクのパブリケーションを」組み込みました:

該当製品

修正済みソフトウェア

Cisco IOSソフトウェア、H.323 パケットのための H.323、または H.225.0 呼出し シグナリングを実行する設定される NAT のために SIP のための NAT をサポートし、Cisco デバイスは影響を受けています。

NAT がデバイスへの Cisco IOS デバイス ログインで確かめ有効になる、**show ip nat statistics** コマンドを発行するためかどうか。次の例は NAT で設定されるデバイスを示したものです：

```
Router#show ip nat statistics
```

```
Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135 Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool mypool refcount 2
  pool mypool: netmask 255.255.255.0
    start 192.168.10.1 end 192.168.10.254
    type generic, total addresses 14, allocated 2 (14%), misses 0
```

また、管理者は **show running-config** を使用できます | NAT がルータ インターフェイスで有効になったかどうかを確認する **ip nat** コマンドを含んで下さい。

ルータで有効になるべき NAT に関しては **IP NAT イネーブル interface** コマンドがある場合 **ip nat inside** がおよび **ip nat outside** コマンドは異なるインターフェイスに [NAT 仮想インターフェイス](#) の場合には、ある。

ソフトウェアを判別するためにデバイスに Cisco IOS 製品で、ログイン動作するシステムバナーを表示する **show version** コマンドを発行すれば。Cisco IOS ソフトウェアは「インターネットワーク オペレーティング システム ソフトウェア」として識別しますそれ自身をまたは単に「IOS」。出力次の行、「バージョンに」先行しているかっこと Cisco IOS リリース名前間のイメージ名 ディスプレイ。他の Cisco デバイスに **show version** コマンドがありませんし、別の出力を与えないために。

次の例は IOS イメージを実行するデバイスからの出力を示したものです：

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE (fcl)
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
```

<More output removed for brevity>

脆弱性を含んでいないことが確認された製品

明示的に NAT のために設定されない Cisco IOS デバイスは脆弱ではありません。

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

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。

改訂履歴

リビジョン 1.0	2010-Sep-22	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。