

# 巧妙に細工された IP オプションの脆弱性

**Critical** アドバイザリーID : cisco-sa-[CVE-20070124-crafted-ip-option](#)  
初公開日 : 2007-01-24 16:00 [2007-0480](#)  
バージョン 2.0 : Final  
CVSSスコア : [10.0](#)  
回避策 : [Yes](#)  
Cisco バグ ID : [CSCec71950](#)

**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® か Cisco IOS XR ソフトウェアを運営する Cisco ルータおよびスイッチはリモートで開発可能な巧妙に細工された IP オプション サービス拒絶 (DoS) 攻撃に脆弱かもしれません。脆弱性の不正利用は任意のコード実行を可能性としては可能にするかもしれません。脆弱性はインターネット制御メッセージプロトコル (ICMP) パケット、Protocol Independent Multicast バージョン 2 (PIMv2) パケット、Pragmatic General Multicast (PGM) パケット、またはパケットの IP ヘッダーで特定の巧妙に細工された IP オプションが含まれている URL Rendezvous Directory (URD) パケットを処理した後不正利用されるかもしれません。他の IP プロトコルはこの問題から影響を受けません。

シスコでは、該当するお客様用に、この脆弱性に対応する無償ソフトウェアを提供しております。

この脆弱性に対しては、影響を緩和するための回避策があります。

この脆弱性は内部テストの間に検出されました。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-crafted-ip-option> で掲示されます。

## 該当製品

## 修正済みソフトウェア

この問題は Cisco IOS か Cisco IOS XR ソフトウェアを実行し、バージョン 4 (IPv4) パケットを Internet Protocol (IP) 処理するために設定されるすべての Cisco デバイスに影響を与えます。バージョンだけ 6 (IPv6) Internet Protocol (IP) 実行するデバイスは影響を受けていま

せん。

この脆弱性は Cisco IOSソフトウェアのすべての取りはずされたバージョンに、バージョン 9.x を含んで、10.x、11.x および 12.x あります。

この脆弱性は Cisco IOS XR ソフトウェアのすべての取りはずされたバージョンに、バージョン 2.0.X を含んで、3.0.X および 3.2.X あります。

修正済みソフトウェア 下記の表にリストされているバージョン前の Cisco IOS または Cisco IOS XR のすべてのバージョンはこの脆弱性に敏感かもしれません。

Cisco 製品で稼働しているソフトウェアを確認するには、デバイスにログインし、**show version** コマンドを発行してシステム バナーを表示します。Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。出力次の行で、イメージ名は「バージョンに」先行しているか、こと IOSリリース名の間で表示する。Cisco IOS XR ソフトウェアは「バージョン」およびバージョン番号に先行している「Cisco IOS XR ソフトウェア」としてそれ自身を識別します。その他の Cisco デバイスには **show version** コマンドがないか、異なる出力が返されます。

次の例は C7200-IS-M のインストール済みイメージ名前と Cisco IOS Release 12.2(14)S16 を実行する Cisco製品を指定したものです：

```
Cisco Internetwork Operating System Software  
IOS (tm) 7200 Software (C7200-IS-M), Version 12.2(14)S16, RELEASE SOFTWARE (fc1)
```

リリーストレイン ラベルは "12.2" です。

次の例は C7200-IK9S-M のイメージ名と IOS リリース 12.3(7)T12 を実行する製品を示します：

```
Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(7)T12, RELEASE SOFTWARE (fc1)
```

Cisco IOSバナーについてのその他の情報は

<http://www.cisco.com/web/about/security/intelligence/ios-ref.html> で利用できます。

Cisco IOS XR ソフトウェアは microkernel ベースの分散オペレーティング システム インフラストラクチャを使用する Cisco IOSソフトウェア ファミリーのメンバーです。Cisco IOS XR は Carrier Routing System だけ 1 ( CRS-1 ) および Cisco XR 12000 シリーズ ルータを on Cisco 実行します。

Cisco IOS XR についてのその他の情報は

<http://www.cisco.com/en/US/products/ps5845/index.html> で利用できます

次の例は Cisco IOS XR リリース 3.3.0 を実行する Cisco製品を指定するかどれが **show version** コマンドからの部分的な出力を示したものです：

```
RP/0/RP0/CPU0:router#show version  
Cisco IOS XR Software, Version 3.3.0
```

## 脆弱性を含んでいないことが確認された製品

Cisco IOS および Cisco IOS XR ソフトウェアの稼動していない Cisco 機器は影響を受けません。CatOS ソフトウェアはこの問題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

Revision 1.5	2009- January- 09	不正利用事例と公式発表 セクションを DEC 2008 無秩序通信会議で学ばれた情 報を示すためにアップデートしました
リビ ジヨ ン 1.4	2007- April-22	回避策 > レシーブ ACL セクションへの 更新。 ソフトウェア バージョン および 修正 表および追加された New エントリ 12.3JL の更新済 12.1EO および 12.2BC エントリ。
リビ ジヨ ン 1.3	2007- February -02	ソフトウェア バージョン および 修正 表の更新済 12.0W および 12.1EO エン トリ。
リビ ジヨ ン 1.2	2007- January- 27	更新済 Cisco IOSソフトウェア 表。
リビ ジヨ ン 1.1	2007- January- 25	ソフトウェア バージョン および 修正 セクションでは、追加されたパッケー ジ インストールは Cisco IOS XR バー ジョンテーブルに情報を囲みます。
リビ ジヨ ン 1.0	2007- January- 24	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。