Cisco IOSソフトウェア Internet Group Management Protocol（IGMP）サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20100922-igmp

初公開日 : 2010-09-22 16:00

最終更新日 : 2012-09-21 19:13

バージョン 1.1 : Final

CVSSスコア : 7.1

回避策 : Yes

Cisco バグ ID : CSCte14603

CVE-2010-2830

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® ソフトウェアおよび Cisco IOS XE ソフトウェアのインターネット グループ管理プロトコル（IGMP）バージョン 3 実装の脆弱性はリモート非認証攻撃者により影響を受けたデバイスのリロードを引き起こすことを可能にします。 この脆弱性が繰り返し悪用されると、持続的なサービス拒否（DoS）状態になる可能性があります。 Cisco はこの脆弱性に対処する無償のソフトアップデートをリリースしました。

このアドバイザリは 922-igmp 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。 アドバイザリの 5 つは Cisco IOSソフトウェアの脆弱性に対処し、1 つのアドバイザリは Cisco Unified Communications Manager の脆弱性に対処します。 各アドバイザリには、そのアドバイザリ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:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

該当製品

修正済みソフトウェア

次の製品は、この脆弱性に該当します。

- Cisco IOS ソフトウェア
- Cisco IOS XE ソフトウェア
  Cisco 製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、機器にログインし show version コマンドを実行してシステムバナーを表示させます。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステムバナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他の Cisco 機器では、 show version コマンドがない場合や、表示が異なる場合があります。
  次の例は C1841-ADVENTERPRISEK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 12.4(20)T を実行している Cisco製品を指定したものです:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```

  Cisco IOS ソフトウェア リリース 命名規則についてのその他の情報は白書で利用できます: 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。Cisco IOS XR ソフトウェアはこの脆弱性から影響を受けません。

Cisco IOS の IGMP バージョン 1、IGMP バージョン 2 および IPv6 マルチキャスト リスナー ディスカバリプロトコル（MLD）機能および Cisco IOS XE ソフトウェアはこの脆弱性から影響を受けません。

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、単独の転載や意訳を施した場合、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。