

# Cisco Catalyst 6000、6500 シリーズおよび Cisco 7600 シリーズ NAM ( Network Analysis Module ) の脆弱性

**Critical**    アドバイザリーID : [cisco-sa-20070228-nam](#)                      [CVE-2007-1257](#)  
初公開日 : 2007-02-28 16:00  
バージョン 1.1 : Final  
CVSSスコア : [10.0](#)  
回避策 : [Yes](#)  
Cisco バグ ID : [CSCsd75273](#) ,  
[CSCse52951](#)

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

Network Analysis Module がインストールされている Cisco Catalyst 6000、6500 シリーズ、および Cisco 7600 シリーズには脆弱性があります。この脆弱性が悪用されると、攻撃者がシステムの完全制御を取得できる可能性があります。この脆弱性に該当するのは、NAM がインストールされている Cisco Catalyst システムのみです。この脆弱性は Internetwork Operating System ( IOS ) または Catalyst Operating System ( CatOS ) を実行しているシステムに該当します。

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。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070228-nam> で掲示されます。

## 該当製品

### 修正済みソフトウェア

この脆弱性は、NAM がインストールされている Catalyst 6000、6500 シリーズ、および Cisco 7600 シリーズに該当します。NAM がインストールされているシステムは、`show module` コマンドによって確認できます。この出力では、NAM が WS-SVC-NAM-1、WS-SVC-NAM-2、

または WS-X6380-NAM として表示されています。

この脆弱性は、IOS または CatOS を実行しているシステムに該当します。

次に、NAM-2 がインストールされているシステムの出力例を示します。

```
Cat6k#show module
Mod Ports Card Type                               Model                               Serial No.
-----
 1     2 Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE                    SAL06417E23
 3    48 48 port 10/100 mb RJ-45 ethernet      WS-X6248-RJ-45                     SAD050108R4
 5     8 8 port 1000mb ethernet                 WS-X6408-GBIC                      SAD041300CL
 6     8 Network Analysis Module                 WS-SVC-NAM-2                       SAD093002AM
```

## 脆弱性を含んでいないことが確認された製品

この脆弱性に該当するその他の Cisco 製品は現在のところ見つかりません。

### 改訂履歴

リビジョン 1.1	2007年3月 15日	CatOS リリース 7.6(20) の 入手可能日を更新
リビジョン 1.0	2007年2月 28日	初回公開リリース

### 利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。