# シスコ セキュリティ アドバイザリ： Cisco Catalyst Enable Password Bypass の脆弱性

severity

**アドバイザリーID :** cisco-sa-20030424-catos

**初公開日 :** 2003-04-24 08:00

**バージョン 1.4 :** Final

**回避策 :** Yes

**Cisco バグ ID :**

**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

7.5(1) リリースのイネーブル モードへの Cisco Catalystソフトウェア割り当て不正アクセス。 最初のアクセスが認められれば、アクセスはパスワードなしで高レベル enable モードのために得ることができます。 この問題はバージョン 7.6(1)で解決されます。 脆弱なリリースを持つ顧客はできるだけ早くアップグレードするように勧められます。

この問題は Cisco バグ ID CSCea42030 で文書化されています。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030424-catos で掲示されます。

## 該当製品

### 修正済みソフトウェア

- Cisco Catalyst 4000 （ Catalyst OS ）
- Cisco Catalyst 6000 （ Catalyst OS ）
- Cisco Catalyst 6500 （ Catalyst OS ）

### 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。

## 改訂履歴

| | | |
|---|---|---|
| リビジョ | 24-April- | 初回公開リリース |

| | | |
|---|---|---|
| ン 1.0 | 2003 | |
| リビジョン 1.1 | 24-April-2003 | 「不正利用事例と公式発表」セクションの下の追加された説明。 |
| リビジョン 1.2 | 25-April-2003 | 問題を報告した追加された顧客名、不正利用に関する訂正された詳細、および AAA サービスのアップデートされた回避策情報。 |
| リビジョン 1.3 | 07-May-2003 | AAA設定例への追加されたリンク。 |
| リビジョン 1.4 | 05-January-2005 | 回避策 セクションの設定 TACACS+、RADIUS および Kerberos Catalyst スイッチ 文書 URL を on Cisco アップデートしました。 |

## 利用規約