

Cisco Clean Access 非認証 API アクセス

severity アドバイザリーID : cisco-sa-
20050817-cca [CVE-
2005-
2631](#)
初公開日 : 2005-08-17 16:00
バージョン 1.0 : 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

Cisco Clean Access (CCA) は自動的に検出することができるソフトウェアソリューション隔離し、ネットワークにアクセスするように試みる感染させるか、または脆弱なデバイスをきれいにするためにです。

CCA はアーキテクチャの一部として Application Program Interface (API) が含まれています。API メソッドを呼び出している間認証の欠如は攻撃者がチェックするセキュリティ態勢をバイパスすることを可能にすることができ、ユーザ向けの assigned roles を、接続解除 ユーザ変更し、また設定されたユーザの情報の漏えいに導く場合があります。

Cisco はこの脆弱性に対処するためにフリーソフト パッチを使用できるようにしました。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050817-cca> で掲示されます。

該当製品

修正済みソフトウェア

- CCA リリース 3.3.0 に 3.3.9
- CCA リリース 3.4.0 に 3.4.5
- CCA リリース 3.5.0 に 3.5.3

脆弱性を含んでいないことが確認された製品

以下の製品は確認された脆弱です:

- 3.3.0 以前の CCA リリース
- CCA リリース 3.5.4 またはそれ以降

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	2005-August-17	初期リリース
-----------	----------------	--------

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。