

Kerberos 5 実装の脆弱性

severity	アドバイザーID : cisco-sa-20040831-krb5	CVE-2004-0772
	初公開日 : 2004-08-31 18:30	
	バージョン 1.0 : Final	CVE-2004-0644
	回避策 : Yes	CVE-2004-0643
	Cisco バグ ID :	CVE-2004-0642

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 VPN 3000 シリーズ コンセントレータに影響を与える [マサチューセッツ工科大学 \(MIT\) Kerberos 5](#) 実装の 2 脆弱性は MIT Kerberos チームによって発表されました。

Kerberos Key Distribution Center (KDC) に対してユーザを認証する Cisco VPN 3000 シリーズ コンセントレータはリモート コード 実行とサービス拒否 (DoS) 不正侵入に脆弱かもしれません。Cisco はこれらの問題を提起するためにフリーソフトを使用できるようにしました。

Kerberos Key Distribution Center (KDC) に対してユーザを認証しない Cisco VPN 3000 シリーズ コンセントレータは影響を与られません。

これらの脆弱性の不正利用は報告されませんでした。

このアドバイザーは [831-krb5](#) で利用できます。

該当製品

修正済みソフトウェア

以下の製品に MIT Kerberos コードに基づいて Kerberos 5 実装があり、これらの脆弱性から影響を受けます:

- Cisco VPN 3000 シリーズ コンセントレータ。 4.0.5.B 以前のすべての 4.0.x ソフトウェアバージョンおよび 4.1.5.B 以前のすべての 4.1.x ソフトウェアバージョンは脆弱です。 4.0.x 以前のバージョンはそれらが Kerberos 認証をサポートしないので脆弱ではありません。

Kerberos KDC に対してユーザを認証するために設定されるときだけ脆弱性が存在する製品が影響を与えられることに注目して下さい。

脆弱性を含んでいないことが確認された製品

以下の製品に Kerberos 5 サポートがありますが、従って実装は MIT Kerberos に基づいていないし、このアドバイザリで説明されている脆弱性から影響を受けません:

- Cisco IOS^Å® (リリース 11.2 またはそれ以降で利用可能な Kerberos サポート)
- Cisco CatOS

従って以下の製品に Kerberos 5 サポートがないし、これらの脆弱性から影響を受けません:

- Cisco PIX ファイアウォール
- Cisco Catalyst 6500 シリーズおよび Cisco 7600 シリーズ ルータのための Cisco Firewall サービス モジュール (FWSM)

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	2004-August-31	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。