Windows NT サーバのための CiscoSecure ACS の多重 脆弱点

severity

アドバイザリーID : cisco-sa-20000921-secure-acs-nt

初公開日 : 2000-09-21 17:00

バージョン 1.3 : 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

多重 脆弱点は Windows NT サーバのための CiscoSecure ACS で特定および解決されました:

- CSAdmin ソフトウエアモジュールはそれの送信によってクラッシュするために特大 URL 強制することができます。 この問題は Cisco バグ ID **CSCdr68286** として文書化されています。
- Windows NT サーバのための CiscoSecure ACS は不安定状態にそれの送信によって特大 TACACS+ パケット置くことができます。 この問題は Cisco バグ ID **CSCdr51286** として文書化されています。
- イネーブルパスワードは Windows NT サーバのための CiscoSecure ACS がユーザがヌル パスワードがあることを可能にする LDAPサーバと共に使用されるときルータの不正 な特権を得るか、または切り替えるためにバイパスすることができます。 この問題は Cisco バグ ID **CSCdr26113** として文書化されています。

2.1(x) 以前の Windows NT サーバのための CiscoSecure ACS のすべてのリリース、2.3(3)、および 2.4(2) は脆弱です。 これらの問題はリリース 2.4(3) およびすべての後続のリリースで修正されます。 無償アップグレードは下記に示されているようにすべての影響を受けた顧客に提供されます。 アップグレードの代りに、複数の回避策は力がこれらの問題によって課される脅威を最小に すること利用できます。

CiscoSecure ACS for UNIX はこれらの脆弱性から影響を受けません。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20000921-secure-acs-nt で利用できます。

該当製品

修正済みソフトウェア

この文書に説明がある問題は CiscoSecure ACS のリリース 2.1(x)、2.3(3)、および Windows NT サーバ、またすべての以前のリリースのために 2.4(2) にあります。

3 つの問題はすべてリリース 2.4(3) で修理されました。 Windows NT サーバのための CiscoSecure ACS のすべての後続のリリースは修正が含まれています。

脆弱性を含んでいないことが確認された製品

CiscoSecure ACS の以前に述べられたリリースはそれらが Windows NT サーバで動作するときだけ脆弱です。 CiscoSecure ACS for UNIX はとりわけこれらの脆弱性が危険な状態の原因ではないです。

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 1.3	2000-October-20	顧客に TAC に修正済みソフトウェアを入手するために連絡するために依頼するために編集される。
リビジョン 1.2	2000-September-21	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。