

Cisco 6400 NRP2 Telnet脆弱性

severity アドバイザリーID : cisco-sa-20010614-nrp2-telnet
初公開日 : 2001-06-14 15:00
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 6400 アクセス コンセントレータ Node Route Processor 2 (NRP2) モジュールはパスワードが設定されなかったら Telnetアクセスを許可します。正しい応答はパスワードが設定されるまでモジュールへのリモート アクセスを拒否することです。この脆弱性はセキュアなシステムに意図的でないアクセスを得ているユーザという結果に終るかもしれません。

この脆弱性は Cisco バグ ID CSCdt65960 として文書化されています。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010614-nrp2-telnet> で掲示されます。

該当製品

修正済みソフトウェア

12.1(05)DC01 以前の Cisco IOS® リリースを実行する Cisco 6400 NRP2 モジュールはこの脆弱性から影響を受けます。

ソフトウェアリビジョンを、型 `show version` コマンド・ライン プロンプトで確認するため。

脆弱性を含んでいないことが確認された製品

Cisco 6400 NSP および Cisco 6400 NRP1 モジュールはこの脆弱性から影響を受けません。その他のCisco製品は現在この脆弱性から影響を受けるために知られていません。

改訂履歴

リビジョン 1.0	2001-June-14	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。