

Cisco VPN 5000 Client 多重脆弱点

severity アドバイザリーID : cisco-sa-
20020918-vpn5k-vulnerability [CVE-
2002-
1491](#)
初公開日 : 2002-09-18 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

多重脆弱点は Cisco Virtual Private Network (VPN) 5000 クライアントソフトウェアにあります。これらの脆弱性は Cisco バグ ID CSCdx17109 および CSCdy20065 として文書化されています。利用可能ないくつかの回避策がこれらの脆弱性の効果を軽減するためにあります。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020918-vpn5k-vulnerability> で掲示されます。

該当製品

修正済みソフトウェア

DDTS - 説明	該当するリリース
CSCdx17109 - MAC OS VPN 5000 Client パスワードの脆弱性	先の MAC OS VPN 5000 Client リリースより 5.2.2
CSCdy20065 - Linux および Solaris VPN 5000 Client バッファオーバーフローの脆弱性	<ul style="list-style-type: none">先の Linux VPN 5000 Client リリースより 5.2.7先の Solaris VPN 5000 Client リリースより 5.2.8

脆弱性を含んでいないことが確認された製品

Cisco VPN 3000 Client および Cisco VPN Client は影響を受けていません。

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	2002-September-18	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。