

Cisco 侵入防御システム スキャン バイパス の脆弱性

Medium	アドバイザリーID : Cisco-SA-20060920-CVE-2006-4911	CVE-2006-4911
	初公開日 : 2006-09-20 18:13	
	バージョン 1.0 : Final	
	CVSSスコア : 2.3	
	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

5.1(2) 以前の Cisco 侵入防御システム バージョンは非認証を可能にする可能性があるセキュリティ スキャンをバイパスするために脆弱性がリモート攻撃者含まれています。

この脆弱性はきちんとフラグメント化されたパケットを処理する失敗が原因です。非認証はネットワーク要求の送信によって、リモート攻撃者 IPS 検出ルールが引き起こされないようにこの脆弱性を不正利用できます。これは攻撃者が IPS スキャンおよび保護を避けることを可能にすることができ、可能性としてはセキュア ネットワークの悪意のあるトラフィックを通過させることを攻撃者を許可します。

Cisco はそれを訂正する Security Advisory のこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

攻撃者は二次目標に対して不正侵入を遂行するのにこの脆弱性を不正利用するように試みるかもしれませんが、攻撃者がスキャンしないで悪意のあるトラフィックを通過できるので、これは IPS デバイスのような不正侵入を軽減することができません。脆弱性のこの型が攻撃者にネットワークトポロジの親密なナレッジがある目標とされた不正侵入で利用される、可能性が高いといえます。

該当製品

修正済みソフトウェア

次のソフトウェアを稼動するシステムは脆弱です:

5.0(6p2) 前の Cisco IPS 5.0(x) ソフトウェア

Cisco IPS 5.1(x) ソフトウェア前の 5.1(2)

脆弱性を含んでいないことが確認された製品

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

バージョン	説明	Section	ステータス	日付
1.0	初版リリース	該当なし	Final	2006-Sep-20

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。本アドバイザリに関する情報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。