

未確認のSIPインスペクションの脆弱性

Informational アドバイザリーID : cisco-sa-20060815-sip
初公開日 : 2006-08-15 16:00
バージョン 1.0 : Final
回避策 : No Workarounds available
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

これは、Cisco Product Security Incident Response Team(PSIRT)が、最近のBlack Hat USA 2006のブリーフィングで最初に公開した潜在的な脆弱性に関して最初に行った回答です。「SIPスタックフィンガープリントとスタック差分攻撃」というタイトルのプレゼンテーションで、Hendrik Scholzは、Cisco PIX 500シリーズセキュリティアプライアンスがSession Initiation Protocol(SIP)メッセージのインスペクションを処理する方法に潜在的な脆弱性があることを言及しました。

広範なテストを行った結果、シスコはこの問題を再現できなくなり、Scholz氏の主張を確認できなくなりました。

シスコは、新しい情報が利用可能になった場合に、このSecurity Responseを更新します。

追加情報

Hendrik ScholzがBlack Hat USA 2006 Briefingsでの講演で示した問題は、PIXファイアウォールによるSIPメッセージのインスペクションの処理方法に関連しています。Scholz氏によると、特別に巧妙に細工されたSIPメッセージを受信すると、PIXは内部ネットワーク内の任意のデバイスへのUser Datagram Protocol (UDP ; ユーザデータグラムプロトコル) 接続を開くことができます。この接続により、攻撃者はUDPトラフィックを内部デバイスに送信できるようになります。

プレゼンテーションの前にシスコはこの潜在的な脆弱性に気づいていませんでしたが、シスコはScholz氏と協力して、提示された調査結果を再作成しました。これまで、シスコは、提示された脆弱性の説明と、シスコに対してさらに提供された情報に基づいて、脆弱性のある状況を作成することができませんでした。その結果、不具合は申し立てられていませんが、状況を再現し、主張を検証するために、Scholz氏と協力して作業を続けます。

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト

https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合わせる場合の説明も含まれています。すべての Cisco セキュリティ アドバイザリは、<http://www.cisco.com/go/psirt> から入手できます。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060815-sip>

改訂履歴

バージョン	説明	セクション	日付
リビジョン 1.0	初回公開リリース		2006年8月15日

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。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。