Catalyst 6500およびCisco 7600上のCisco IOSのアクセスコントロールリストバイパスの脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20070926-CVE-2007-5134 **初公開日 :** 2007-09-26 22:30 **最終更新日 :** 2012-07-14 19:51 **バージョン 2.0 :** Final **CVSSスコア :** 5.0 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2007-5134

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

Catalyst 6500およびCisco 7600で稼働するCisco IOSには、認証されていないリモートの攻撃者が設定されたACLをバイパスできる可能性のある脆弱性が存在します。

この脆弱性は、Ethernet Out-of-Band Channel(EOBC)で使用するために予約されているIPアドレスへのトラフィックが、該当デバイスで受け入れられるために存在します。 通常、これらのアドレスはEOBCの外部から到達可能ではないと想定されるため、ACLによって保護されません。 認証されていないリモートの攻撃者は、この脆弱性を不正利用して、公開された管理アドレスを保護するように設定されたACLをバイパスし、スーパーバイザやMulti-layer Switch Feature Card（MSFC；マルチレイヤスイッチフィーチャカード）などのインテリジェントモジュールにパケットを送信する可能性があります。

この脆弱性を不正利用するためにエクスプロイトコードは必要ありません。

シスコは、この脆弱性をセキュリティレスポンスで確認し、更新されたソフトウェアをリリースしました。

この脆弱性は、ハイブリッドモード（スーパーバイザエンジンのCatOSとMSFCのIOS）とネイティブモード（スーパーバイザエンジンとMSFCの両方のIOS）の両方で動作しているCatalyst 6500およびCisco 7000デバイスに影響を与えます。 127.0.0.0/8ネットワークは、RFC 3330で指定されているように、ループバックおよび内部通信用に予約されています。 そのため、このネッ

トワークに向かうトラフィックはパブリックインターネット経由でルーティングされません。 ただし、Ciscoルータで実行されているIOSの一部のデフォルト設定では、このようなトラフィックが信頼できる内部ネットワークを通過できる場合があります。 これを可能にする状況は非常に特殊であり、ほとんどのネットワークで発生する可能性は低いです。これらの要因により、潜在的な攻撃者のプールが大幅に減少します。 この脆弱性を使用して該当デバイスにアクセスするACLをバイパスする攻撃者は、コンフィギュレーションファイルの変更などのアクションを実行するために引き続き認証を行う必要があります。

ダウンタイムやソフトウェアのアップグレードを行うことなく、この脆弱性を効果的に緩和する方法は複数あります。 高可用性環境の管理者は、ACLまたはコントロールプレーンポリシング(CoPP)を使用して、不要なトラフィックがインテリジェント管理カードに到達するのを防ぐことをお勧めします。 管理者は、スケジュールされた次の計画的な停止の際に、これらのデバイスで実行されているソフトウェアを更新することを推奨します。

この脆弱性は、12.2(33)SXHのリリースで解決されています。

該当製品

シスコは、Cisco Bug ID CSCek49649(Cisco-sr-20070926-lb)に対応するため、セキュリティ応答を再リリースしました。

脆弱性のある製品

Cisco Catalyst 6500およびCisco 7600デバイスで次のバージョンのCisco IOSが稼働しているシステムには、脆弱性が存在します。

12.2(18r)SX
12.2(99)SX
12.2(18)ZU
12.2(18)ZY
12.2(18)IXA
12.2(18)IXB
12.2(18)IXC
12.2(18)IXD
12.2(18)SXD
12.2(18)SXE
12.2(18)SXF
12.3(18r)S
12.3(18r)SX

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。

回避策

影響を受けるデバイスへのアクセスを制限するには、Cisco Security Responseで指定されているようにACLを実装することを推奨します。

CoPPを使用して、管理トラフィックを許可されたパスとワークステーションだけに制限することを推奨します。

悪意のあるトラフィックがネットワークに入り込まないように、エッジデバイスにブラックホールルートを配置することを検討する可能性があります。

Cisco Applied Intelligenceチームは、この脆弱性を悪用しようとする攻撃を識別して緩和するために、更新されたソフトウェアを適用する前に管理者を導く次の関連ドキュメントを作成しました。cisco-air-20070926-lb

修正済みソフトウェア

有効な契約を結んでいるシスコのお客様は、CiscoのSoftware Centerからアップデートを入手できます。契約を結んでいないシスコのお客様は、Cisco Technical Assistance Center(TAC)に1-800-553-2447または1-408-526-7209で連絡するか、tac@cisco.comに電子メールでアップグレードを入手できます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20070926-CVE-2007-5134

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2007年9月26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。

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。