

Cisco IOS XRソフトウェアのSNMPにおけるDoS脆弱性

Medium	アドバイザーID : Cisco-SA-20130523-CVE-2013-1204	CVE-2013-1204
	初公開日 : 2013-05-23 16:59	
	バージョン 1.0 : Final	
	CVSSスコア : 5.0	
	回避策 : No Workarounds available	
	Cisco バグ ID : CSCug80345	

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 IOS XRソフトウェアのSNMPプロセスの脆弱性により、認証されていないリモートの攻撃者が該当プロセスのリロードと、プロセスに影響を与える限定的なメモリリークを引き起こす可能性があります。

この脆弱性は、割り当てられたメモリを解放しないことに起因します。攻撃者は、該当デバイスのSNMPポート162に大量のUDPパケットを送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はSNMPプロセスのみに影響する限定的なメモリリークを引き起こす可能性があります。攻撃者は、該当プロセスのリロードを繰り返す可能性もあります。

シスコはセキュリティ通知で脆弱性を確認しましたが、ソフトウェアアップデートは利用できません。

この脆弱性をエクスプロイトするには、攻撃者が該当ソフトウェアに巧妙に細工された要求を送信するために、信頼できる内部ネットワークへのアクセスを必要とする可能性があります。このアクセス要件により、不正利用が成功する可能性が制限される可能性があります。

シスコはCVSSスコアを通じて、機能不正利用コードが存在することを示していますが、このコードが一般に公開されているかどうかは不明です。

該当製品

シスコは、[CVE-2013-1204](#)のリンクで、Bug ID [CSCug80345](#)のセキュリティアドバイザリをリ

リリースしました。

脆弱性のある製品

このアラートが最初に公開された時点では、Cisco IOS XRソフトウェアバージョン4.3.0には脆弱性が存在していました。Cisco IOS XRの新しいバージョンも影響を受ける可能性があります。

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

今後のアップデートやリリースについては、ベンダーに連絡することを推奨します。

信頼できるユーザだけにネットワークアクセスを許可することを推奨します。

IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけに該当システムへのアクセスを許可することを検討することもできます。

影響を受けるシステムを監視することを推奨します。

ネットワーク上のアクティビティを理解することで、潜在的なセキュリティインシデントを特定するために使用できる情報と可視性が得られます。組織は、デバイスからのイベントをログに記録し、記録されたデータを確認して、異常または悪意のあるアクティビティに関する洞察を提供する必要があります。ロギングのベストプラクティスについては、『[Cisco Guide to Harden Cisco IOS Devices](#)』を参照してください。

セキュリティ関連のネットワークアクティビティのネットワークトラフィックを監視することをお勧めします。NetFlowはそのようなアクティビティを識別します。NetFlowの設定の詳細については、「[Cisco IOS NetFlowの概要 – 技術的概要](#)」を参照してください。

ネットワークデバイスへの不正な直接通信を防止することが重要です。偵察攻撃やサービス拒否攻撃から保護するために、ネットワークインフラストラクチャを宛先とするネットワークトラフィックを制限します。設定の詳細については、『[コアの保護：インフラストラクチャ保護ACL](#)』を参照してください。

修正済みソフトウェア

これらの問題の修正を含むソフトウェアバージョンへのアップグレードを希望するお客様は、通常のサポートチャネルにお問い合わせください。Cisco Security Noticeで公開された問題に対しては、無償のソフトウェアアップデートは提供されません。Ciscoのお客様は、Cisco Technical Assistance Center(TAC)に1-800-553-2447または1-408-526-7209で問い合わせるか、

tac@cisco.comで電子メールを介して問い合わせることができます。

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-20130523-CVE-2013-1204>

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	2013年5月23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。