Cisco Security Agent for Linuxのポートスキャンにおける DoS

アドバイザリーID : cisco-sa-20061025-csa CVE-2006-5553
初公開日 : 2006-10-25 16:00
バージョン 1.0 : Final
CVSSスコア : 2.3
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

Cisco Security Agent(CSA)for Linuxには、ポートスキャンに関連するサービス拒否(DoS)の脆弱性があります。脆弱性のあるバージョンのCSAを実行しているシステムに対してポートスキャンを実行すると、システムが応答しなくなる可能性があります。Cisco Unified CallManager(CUCM)およびCisco Unified Presence Server(CUPS)には、脆弱性のあるCSAバージョンが付属しています。

この脆弱性には回避策があります。シスコでは、該当するお客様用に、この脆弱性に対応する無償ソフトウェアを提供しております。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20061025-csa で公開されています。

該当製品

脆弱性のある製品

次のCSAバージョンには、ポートスキャンの問題に対する脆弱性があります。

- ホットフィックス4.5.1.657より前のLinux（スタンドアロンおよびマネージド）用CSAバージョン4.5
- ホットフィックス5.0.0.193より前のLinux（スタンドアロンおよびマネージド）用CSAバージョン5.0

次のシスコ製品には、スタンドアロンCSA for Linuxバージョンが含まれており、この問題に対する脆弱性もあります。

- Cisco Unified CallManager(CUCM)5.0バージョン(5.0(4)および5.0(4a)を含む)
- Cisco Unified Presence Server(CUPS)1.0バージョン、1.0(2)を含む

脆弱性を含んでいないことが確認された製品

次のバージョンのCSAエージェントには、ポートスキャンの問題に対する脆弱性はありません。

- Linux用CSAバージョン5.1（スタンドアロンおよびマネージド）
- Windows用のすべてのCSAバージョン（スタンドアロンおよびマネージド）
- Solaris用のすべてのCSAバージョン（スタンドアロンおよびマネージド）

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。

詳細

Cisco Security Agent(CSA)は、サーバおよびデスクトップコンピューティングシステムを脅威から保護します。CSA for Linuxは、ネットワークポートスキャンの識別中にトリガーされる可能性があるサービス拒否攻撃に対して脆弱です。特定のオプションを指定してポートスキャンを実行すると、システムリソースの過度の消費が発生し、サービス拒否が発生する可能性があります。脆弱性のあるシステムへのネットワークアクセスを信頼できるネットワークに制限することで、この脆弱性を緩和できます。この問題は、Linuxオペレーティングシステムの問題ではありません。他のオペレーティングシステム(Windows、Solaris)用のCSAバージョンは、この脆弱性の影響を受けません。この問題は、Cisco Bug ID CSCse98684(登録ユーザ専用)に記述されています。

Cisco Unified CallManager 5.0バージョン(5.0(4)および5.0(4a)を含む)には、脆弱性のあるバージョンのCSAが付属しています。新しいCallManager Options Package(COP)ファイルを使用して、CallManager 5.0(4)のCSAバージョンを更新できます。CallManagerの今後のバージョンには、更新されたCSAバージョンが含まれる予定です。この問題は、Cisco Bug ID CSCse97601(登録ユーザ専用)に記述されています。

Cisco Unified Presence Server(CUPS)1.0バージョン(1.0(2)を含む)には、脆弱性のあるバージョンのCSAが付属しています。CUPS 1.0(2)のCSAバージョンを更新するための新しいCOPファイルが用意されています。CUPSの将来のバージョンには、更新されたCSAバージョンが含まれます。この問題は、Cisco Bug ID CSCsg40052(登録ユーザ専用)に記述されています。

回避策

Linuxポートスキャンの脆弱性は、CSA Management Center(CSAMC)コンソールから管理対象エージェントのNetshieldルールを無効にすることで回避できます（スタンドアロンおよびCUCM/CUPSエージェントでは不可能）。この回避策を使用する場合、追加のネットワークDoS攻撃を受ける可能性があるため、管理者は注意が必要です。Netshieldルールを無効にしても、CSAはバッファオーバーフローやその他の悪意のあるアクティビティに対する保護を提供しま

す。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Linux向けCSA

該当するソフトウェア バージョン	修正済みソフトウェアバージョン
4.5.1.657より前のCSAホットフィックス	CSAホットフィックス 4.5.1.657
5.0.0.193より前のCSAホットフィックス	CSAホットフィックス 5.0.0.194 *

* CSA Hotfix 5.0.0.194は、CSA Hotfix 5.0.0.193を廃止したものです。

修正済みのCSAソフトウェアは、http://www.cisco.com/pcgi-bin/tablebuild.pl/csahf-crypto?psrtdcat20e2からダウンロードできます。

CUCM/CUPS

該当するソフトウェア バージョン	修正済みソフトウェアバージョン
5.0(4)および5.0(4a)を含むCUCM 5.0バージョン	CUCM 5.0(4)および5.0(4a)とCSA COPのアップグレード
CUPS 1.0バージョン	CSA COPアップグレード付

(1.0(2)を含む)	きCUPS 1.0(2)

CUCM COPファイル(platform-csa-4.5.1-657.1.cop.sgn)とインストール手順は、http://www.cisco.com/pcgi-bin/tablebuild.pl/cmva-3des?psrtdcat20e2からダウンロードできます。

CUPS COPファイル(CUPS-1.0.2-CSA-4.5.1-657.1.i386.cop.sgn)およびインストール手順は、http://www.cisco.com/pcgi-bin/tablebuild.pl/cups-10?psrtdcat20e2からダウンロードできます。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

この脆弱性はシスコ内部で発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20061025-csa

改訂履歴

リビジョン 1.0	2006年10月25日	初回公開リリース

利用規約

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。