Cisco Network Admission Controlの共有秘密鍵に関する脆弱性

アドバイザリーID : cisco-sa-20080416-nac CVE-2008-1155
初公開日 : 2008-04-16 16:00
バージョン 1.1 : Final
CVSSスコア : 10.0
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 Network Admission Control（NAC）アプライアンスには、Cisco Clean Access Server（CAS）と Cisco Clean Access Manager（CAM）との間で使用している共有秘密鍵を攻撃者が入手できるという脆弱性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080416-nac で公開されています。

該当製品

脆弱性のある製品

次の表に、この脆弱性の影響を受けるすべてのCisco NACアプライアンスソフトウェアバージョンを示します。

NACソフトウェアリリース	脆弱性のあるバージョン
3.5.x	すべての3.5.xバージョン
3.6.x	3.6.4.4より前のすべての3.6.xバ

	ージョン
4.0.x	4.0.6より前のすべての4.0.xバージョン
4.1.x	4.1.2より前のすべての4.1.xバージョン

脆弱性を含んでいないことが確認された製品

3.6.xトレインのCisco NACアプライアンスソフトウェアバージョン3.6.4.4以降、4.0.xトレインの4.0.6以降、4.1.xトレインの4.1.2以降には脆弱性はありません。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 NACアプライアンスソリューションを使用すると、ネットワーク管理者は、有線、ワイヤレス、およびリモートのユーザとそのマシンに対して、ユーザのネットワークへの接続を許可する前に、認証、許可、評価、および修正を行うことができます。このソリューションは、マシンがセキュリティポリシーに準拠しているかどうかを確認し、ネットワークへのアクセスを許可する前に脆弱性を修正します。

Cisco NACアプライアンスには脆弱性が存在するため、攻撃者はネットワークを介して送信されるエラーログからCASとCAMで使用される共有秘密を取得できます。この情報を取得すると、攻撃者はネットワークを介してリモートでCASを完全に制御できるようになります。

この脆弱性は、Cisco Bug ID CSCsj33976 (登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2008-1155が割り当てられています。

回避策

この脆弱性に対する回避策はありません。

修正済みソフトウェア

次のソフトウェアテーブル（下記）の各行には、この脆弱性に対する修正を含む最初のリリースが記載されています。これらは「First Fixed Release」列に示されています。特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。このようなリリースは、少なくとも、示されているリリース以上（最初の修正リリース ラベル以上）にアップグレードしてする必要があります。

該当するリリース	第 1 修正済みリリース
NACアプライアンスソフトウェアバージョン3.5.x	脆弱性あり – TACに連絡
NACアプライアンスソフトウェアバージョン3.6.x	3.6.4.4
NACアプライアンスソフトウェアバージョン4.0.x	4.0.6
NACアプライアンスソフトウェアバージョン4.1.x	4.1.2

NACアプライアンスソフトウェアはhttp://www.cisco.com/tacpage/sw-center/ciscosecure/cleanaccess.shtmlからダウンロードできます。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。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

この問題は、シスコの社内テストで発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080416-nac

改訂履歴

リビジョン 1.1	2008年4月25日	CSCsj33976のCVSSリンクを更新。
リビジョン 1.0	2008年4月16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。