Cisco Network Admission Control 共有秘密脆弱性

Critical

アドバイザリーID : cisco-sa-20080416-nac

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 :

CVE-2008-1155

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。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080416-nac で掲示されます。

該当製品

脆弱性のある製品

次 の テーブルはすべてをこの脆弱性から影響を受けるソフトウェア バージョン Cisco NAC アプライアンス（Clean Access）リストします。

NAC ソフトウェア リリース	脆弱なバージョン
3.5.x	すべての 3.5.x バージョン
3.6.x	3.6.4.4 以前のすべての 3.6.x バージョン
4.0.x	4.0.6 以前のすべての 4.0.x バージョン
4.1.x	4.1.2 以前のすべての 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

Cisco NAC アプライアンス（Clean Access）3.6.x トレインのソフトウェア バージョン 3.6.4.4 およびそれ以降; 4.0.x トレインの 4.0.6 およびそれ以降; そして 4.1.x トレインの 4.1.2 およびそれ以降は脆弱ではないです。 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（Clean Access）ソリューションはネットワーク管理者が認証することを可能にし、ネットワークにユーザを許可する前に、ワイヤレスおよびリモートユーザおよびマシン配線される remediate 承認し、評価し。 ソリューションはマシンがセキュリティポリシーと対応である識別し、アクセスを許可する前にネットワークに脆弱性をかどうか修復します。

攻撃者が共有秘密を得ることを可能にすることができるで Cisco NAC アプライアンス（Clean Access）存在 する脆弱性はネットワークに送信されるエラーログからの CAS および CAM によって使用しました。 この情報を得ることはネットワークの CAS の完全な制御をリモートで得ることを攻撃者が可能にする可能性があります。

この脆弱性 Cisco バグ ID CSCsj33976（登録ユーザのみ）で文書化されています、よくある脆弱性および公開（CVE）識別子 CVE-2008-1155 は割り当てられました。

セキュリティ侵害の痕跡

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）の各行は最も早い可能性のある リリースを記述しますこの脆弱性のための修正が含まれている。 これらは「最初修正済みリリース」カラムで示されています。 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（Clean Access）ソフトウェア バージョン 3.5.x	脆弱- TAC に連絡して下さい
NAC アプライアンス（Clean	3.6.4.4

Access) ソフトウェア バージョン 3.6.x	
NAC アプライアンス (Clean Access) 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 (Clean Access) ソフトウェア バージョン 4.1.x	4.1.2

http://www.cisco.com/tacpage/sw-center/ciscosecure/cleanaccess.shtml からソフトウェアを NAC アプライアンス (Clean Access) ダウンロードできます。 ソフトウェアのアップグレードを検討する際には、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

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。

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の公示か不正利用に気づいていません。

この問題は内部テストによる Cisco によって検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080416-nac

改訂履歴

リビジョン 1.1	2008-April-25	CSCsj33976 への更新済 CVSS リンク。
リビジョン 1.0	2008-April-16	初回公開リリース

利用規約

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。