

Cisco AnyConnect セキュア モビリティ クライアント WebLaunch セッション ハイジャック脆弱性

Medium	アドバイザーID : Cisco-SA-20120809-CVE-2012-2500	CVE-2012-2500
	初公開日 : 2012-08-09 20:55	
	バージョン 1.0 : Final	
	CVSSスコア : 4.3	
	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 AnyConnect セキュア モビリティ クライアントは非認証を可能にする可能性がある攻撃者が機密情報を代行受信することを可能にする可能性がある WebLaunch セッションを乗っ取るために脆弱性がリモート攻撃者含まれています。

脆弱性は WebLaunch 機能を使用しながらチェックする X.509 証明書で証明書名前を行う障害が原因です。非認証はユーザの巧妙に細工された X.509 証明書を受け入れる悪意のある Web ページにアクセスするように確信によって、リモート攻撃者脆弱性を不正利用する可能性があります。成功すれば、攻撃者はさらなる攻撃を行なうのに使用する可能性がある機密情報の公開という結果に終る可能性がある WebLaunch セッションを代行受信する可能性があります。

Cisco はこの脆弱性およびリリースされたソフトウェア アップデートを確認しました。

この脆弱性のエクスプロイトはユーザー操作を必要とするかもしれませんが。攻撃者はユーザを正規のサイトのために有効ように表示されるかもしれない証明書を使用して悪意のある Web サイトにアクセスするように確信させる可能性があります。さらに、ユーザは IPsec に使用している Cisco AnyConnect セキュア モビリティ クライアントによって攻撃者がこの脆弱性を不正利用するベクトルがあることができるように接続する必要があります。

巧妙に細工された X.509 証明書を入れることを攻撃者は必要とする内部へのアクセスが、プライベート ネットワーク可能性が高いといえます。この要件は不正侵入の可能性を制限するかもしれ

ません。

Cisco は CVSS スコアを通してことを proof-of-concept エクスプロイト コード存在示します; ただし、コードは共用利用可能であると知られていません。

該当製品

Cisco は次のリンクで Cisco バグ ID [CSCtz29470](#) に関するリリース ノートを発表しました:
[Cisco AnyConnect セキュア モビリティ クライアントのためのリリース ノート](#)

脆弱性のある製品

3.0.08057 以前の Cisco AnyConnect セキュア モビリティ クライアント バージョンは脆弱です。

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

管理者は適切な更新を加えるように助言されます。

管理者は信頼されたユーザだけネットワーク アクセスをアクセスできることを許可するために助言されます。

管理者は特権ユーザだけ管理システムにアクセスすることを許可するために助言されます。

管理者は影響を受けたシステムを監視するように助言されます。

修正済みソフトウェア

アクティブな契約を持つ Cisco カスタマは次のリンクで Software Center を通して更新を入手できます: [Cisco](#)。契約のない Cisco カスタマは 1-800-553-2447 か 1-408-526-7209 でまたは tac@cisco.com で E メールで Cisco Technical Assistance Center にコンタクトをとって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) では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

URL

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2012-Aug-09

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。