Cisco Secure Desktop リモート クロスサイト スクリプティング脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20100201-CVE-2010-0440 **初公開日 :** 2010-02-01 19:54 **最終更新日 :** 2012-07-14 14:25 **バージョン 4.0 :** Final **CVSSスコア :** 4.3 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2010-0440

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 Secure Desktop は非認証を可能にする可能性があるクロスサイト スクリプティング攻撃を行なうために脆弱性がリモート攻撃者含まれています。

脆弱性はターゲットとされたユーザの影響を受けた製品の Webインターフェイスに HTTP ポスト要求を入れるように設計されている悪意のある Webサイトを参照するように確信によって非認証 Cisco Secure Desktop.Â の入力サニタイズの欠如が原因、リモート攻撃者この脆弱性を不正利用する可能性がありますです。ターゲットとされたユーザが悪意のあるページを参照すれば Â は、攻撃者影響を受けたサイトのセキュリティ コンテキストのユーザのブラウザの任意スクリプト コードを実行する可能性があります。

Proof-of-concept コードは共用利用可能です。

Cisco はこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

この脆弱性を不正利用するために、攻撃者はターゲットとされたユーザを悪意のある Webサイトを参照するように確信させる必要があります。 エクスプロイトを行うことは多分攻撃者が通信の E メール、インスタント メッセージ、または別の形式によってターゲットとされたユーザの送信のような社会工学作戦を、サイトへのリンク使用するように要求します。

Cisco はこの脆弱性を検出するために Matias パブロ Brutti およびコア セキュリティ技術からの Ernesto Alvarez に感謝することを望みます。

行った Cisco Secure Desktop 3.5 の変更をが理由で、ASA ファームウェアのより古いバージョンのしかし Cisco Secure Desktop 3.5 またはそれ以降の Cisco ASA はこの脆弱性から影響を受けません。

問題は Cisco ASA ファームウェアのバージョンのために固定です
8.0(5) およびそれ以降。

該当製品

Ciscoバグ IDÂ CSCsw15646 Â はこの脆弱性に割り当てられました。

脆弱性のある製品

3.5 以前の Cisco Secure Desktop バージョンは脆弱です。 Cisco Secure Desktop は Cisco Secure Desktop 機能が有効である場合だけ Cisco ASA 5500 シリーズ適応性があるセキュリティ Appliances.Â Cisco ASA 機器のコンポーネントです脆弱です。Â Cisco ASA アプライアンス バージョン前 toÂ 8.2(1)、8.1(2.7)、および 8.0(5) 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。

ユーザは疑わしくか認識されないソースからの電子メール メッセージを開かないように助言されます。ユーザが電子メール メッセージに含まれているリンクか添付ファイルは安全であることを確認できなければ Â、それらを開かないように助言されます。

Cisco によって加えられる知性チームは識別を管理者に指示するために次のドキュメントガイドを作成し、軽減は更新済ソフトウェアを加える前にこの脆弱性を不正利用するように試みます: cisco-amb-20060922-understanding-xss

ユーザは非請求リンクが続いてが安全であることを確認する必要があります。

修正済みソフトウェア

Cisco は followingÂ 修正済み バージョンをリリースしました:

Cisco Secure Desktop
バージョン 3.5

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス

バージョン 8.2(1)、8.1(2.7)、および 8.0(5)

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: 契約のない Cisco.Â 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

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20100201-CVE-2010-0440

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2010-Feb-01

利用規約