オンラインヘルプシステムのクロスサイトスクリプティングの脆弱性

アドバイザリーID : cisco-sa-20070315-xss
初公開日 : 2007-03-15 17:00
バージョン 1.2 : Final
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

複数のシスコ製品に配布されているオンラインヘルプシステムのクロスサイトスクリプティング(XSS)の脆弱性は、Fox-ITのErwin Paternotte氏とCassio Goldschmidt氏によって独立してシスコに報告されています。

この脆弱性により、攻撃者は、巧妙に細工された悪意のあるURLにユーザを誘導することに成功すると、ユーザのWebブラウザで任意のスクリプトコードを実行できるようになります。

脆弱性のあるオンラインヘルプシステムが複数のシスコ製品で使用されているため、複数のシスコ製品が影響を受けます。

この応答は、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070315-xssで公開されています。

追加情報

この脆弱性は、特にオンラインヘルプシステムのコンテンツ検索機能に存在します。この機能を使用すると、ユーザはヘルプコンテンツで特定のキーワードを検索できます。検索機能は、HTMLフォームとスクリプトコードによって実装されます。

この脆弱性は、PreSearch.htmlファイル(製品によってはPreSearch.classファイル)内の検索コードによって、ユーザの入力がすべて正しくサニタイズされないことに起因しています。

この脆弱性は、<script>タグと</script>タグで囲まれたスクリプトコードを含む検索キーワードが検索フォームのテキストフィールドに入力されると発生します。場合によっては、最初のテキス

トがサニタイズされていても、それ以降のテキストはサニタイズされないため、最初のテキストの後のスクリプトコードも脆弱性を引き起こす可能性があります。例：「some text <script>alert('I am a script')</script>」

攻撃者がこの脆弱性を悪用できるようにするには、ユーザによる介入が必要です。攻撃者は、悪意のある特別に巧妙に細工されたURLにユーザを誘導できる必要があります。場合によっては、管理または通常の使用のために、製品が提供するWebインターフェイスでユーザを認証する必要があります。

次のシスコ製品はこの脆弱性の影響を受けます（具体的なバージョンを明記しない限り、すべてのバージョンが影響を受けます）。

- Cisco Secure Access Control Server(ACS)for WindowsおよびCisco Secure ACS Solution Engine。すべての4.xバージョンが影響を受けます。4.0より前のバージョンは影響を受けません。Cisco Bug ID CSCsh91761(登録ユーザ専用)。
- Cisco VPN Client.Cisco Bug ID CSCsh52300(登録ユーザ専用)。
- Cisco Unified Personal Communicator.Cisco Bug ID CSCsh91884(登録ユーザ専用)。
- Cisco MeetingPlaceおよびCisco Unified MeetingPlace、エンドユーザおよび管理者のヘルプシステムCisco Bug ID CSCsi12435(登録ユーザ専用)。
- Cisco Unified MeetingPlace Express、エンドユーザ、および管理者のヘルプシステムCisco Bug ID CSCsh91901(登録ユーザ専用)。
- ルータからダイヤルトーンを受けます。Cisco Bug ID CSCsi10405(登録ユーザ専用)。
- Cisco IP Communicator.Cisco Bug ID CSCsh91953(登録ユーザ専用)。
- Cisco Unified Video Advantage（旧Cisco VT Advantage）Cisco Bug ID CSCsh93070(登録ユーザ専用)。
- Cisco Unified Videoconferencing 3545システム、Cisco Unified Videoconferencing 3540シリーズVideoconferencingシステム、Cisco Unified Videoconferencing 3515 MCU、Cisco Unified Videoconferencing 3527 PRIゲートウェイ、Cisco Unified Videoconferencing 3526 PRIビデオ会議ゲートウェイ、およびCisco Unified Videoconferencing Manager。Cisco Bug ID CSCsh93854(登録ユーザ専用)。
- Cisco WAN Manager(CWM)。Cisco Bug ID CSCek71039(登録ユーザ専用)。
- Cisco Security Device Manager(SDM)。Cisco Bug ID CSCsh95009(登録ユーザ専用)。
- Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用Cisco Network Analysis Module（NAM-1およびWS-SVC-NAM-2）Cisco Bug ID CSCsi10818(登録ユーザ専用)。
- モジュラアクセスルータ(Cisco 26xx、26xxXM、28xx、36xx、37xx、38xx)用のCisco Network Analysis Module(NM-NAM)Cisco Bug ID CSCsi10818(登録ユーザ専用)。
- CiscoWorksおよびCiscoWorksと統合されるすべての製品Cisco Bug ID CSCsi10674(登録ユーザ専用)。

  該当するCiscoWorks関連製品には、次のものがあります。

  - IPSセンサーの管理センター

    - セキュリティモニタ
    - CiscoWorks LAN Management Solution
    - ルータ管理の要点
    - 共通サービス
    - デバイス障害マネージャ
    - CiscoView
    - Internetwork Performance Monitor（IPM）
    - キャンパスマネージャ
- Cisco Wireless LAN Solution Engine(WLSE)。Cisco Bug ID CSCsi10982(登録ユーザ専用)。
- Cisco 2006ワイヤレスLANコントローラ(WLC)Cisco Bug ID CSCsi13743(登録ユーザ専用)。
- Cisco Wireless Control System(WCS)Cisco Bug ID CSCsi13763(登録ユーザ専用)。
- VPN 3000シリーズコンセントレータCisco Bug ID CSCsi47620(登録ユーザ専用)。

場合によっては、PreSearch.htmlファイルとPreSearch.classファイルを削除するか名前を変更することで、この脆弱性を排除できます（ファイルが存在する場合は、オペレーティングシステムのファイル検索機能を使用してファイルを検索します）。 この回避策は、ファイルシステムに直接アクセスできないアプライアンスや他の製品には適用されず、これらのファイルを削除したり名前を変更したりすると、製品のオンラインヘルプの内容を検索できなくなることに注意してください。

クロスサイトスクリプティング(XSS)攻撃とこれらの脆弱性を悪用する方法の詳細については、次のURLにある『Cisco Applied Mitigation Bulletin』の「Understanding Cross-Site Scripting (XSS) Threat Vectors」を参照してください。

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20060922-understanding-xss

Cisco PSIRTでは、このドキュメントで説明されている脆弱性の不正利用事例は確認していません。

この問題は、Fox-ITのErwin Paternotte氏とCassio Goldschmidt氏によってシスコに個別に報告されました。当初のレポートは、それぞれCisco CallManagerとCisco VPN Clientに関するものでした。さらに調査を行ったところ、さらに多数の該当製品が見つかりました。この問題に注意を喚起し、問題の協調した開示に向けて協力してくださったErwin Paternotte、Fox-IT、Cassio Goldschmidt氏に感謝いたします。

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト https://sec.cloudapps.cisco.com/security/center/resources/security_vulner

ability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の説明も含まれています。すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070315-xss

改訂履歴

バージョン	説明	セクション	日付
リビジョン 1.2	VPN 3000シリーズコンセントレータを該当製品として追加。		2007 年 4 月 11 日
リビジョン 1.1	Cisco Secure Access Control Server(ACS)for WindowsおよびCisco Secure ACS Solution Engineのバージョン4.0.xも影響を受けます（このドキュメントの元のリリースでは、バージョン4.1のみが影響を受けると誤って記載されていました）。 影響があるのはネットワーク解析モジュール（NAM-1、WS-SVC-NAM-2、およびNM-NAM）であり、モジュールが挿入されているデバイスのオペレーティングシステム（IOSまたはCatOS）ではないことを明確にします。		2007年3月23日

バージョン	説明	セクション	日付
リビジョン 1.0	Fox-ITのErwin Paternotte氏とCassio Goldschmidt氏の協力による最初の一般公開。		2007 年 3 月 15 日

利用規約

本アドバイザリ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。 本アドバイザリ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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、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。

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。