UPnPデバイス向けポータブルSDKにバッファオーバーフローの脆弱性が含まれる

アドバイザリーID : cisco-sa-20130129-upnp
初公開日 : 2013-01-29 20:00
最終更新日 : 2013-02-13 22:34
バージョン 1.2 : Interim
CVSSスコア : 10.0
回避策 : No Workarounds available
Cisco バグ ID : CSCue21578 CSCue21009 CSCue20997 CSCue19318 CSCue21031

CVE-2012-5958

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

ユニバーサルプラグアンドプレイ(UPnP)デバイス向けPortable Software Developer Kit (SDK)には、本来Intel SDK for UPnP Devicesと呼ばれるlibupnpライブラリが含まれています。このライブラリは、悪意のあるSimple Service Discovery Protocol (SSDP)要求を処理する際に発生する複数のスタックベースのバッファオーバーフローに対して脆弱です。このライブラリは、メディアストリーミングやファイル共有アプリケーションに加えて、複数のベンダーのネットワークデバイスで使用されます。これらの脆弱性は、2013年1月29日にCERT Vulnerability Note、VU#922681で公開されました。このドキュメントは http://www.kb.cert.org/vuls/id/922681で参照できます。

シスコでは現在、これらの脆弱性による影響を受ける可能性のある製品を評価中です。このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130129-upnp

該当製品

シスコでは現在、これらのUPnP脆弱性による問題の発生について製品を評価しています。製品の問題に関する最終的な判断が行われた時点で、このアドバイザリの「脆弱性が存在する製品」または「脆弱性を含んでいないことが確認された製品」のセクションにのみ製品が記載されます。これら2つのセクションのいずれにも記載されていない製品は、引き続き評価中です。

脆弱性のある製品

次の製品は、このアドバイザリに記載されている脆弱性の影響を受けます。

- Cisco TelePresence Cシリーズエンドポイント
- Cisco TelePresence System EX シリーズ
- Cisco TelePresence SX20

このセクションは、より詳細な情報が入手可能になると更新されます。

脆弱性を含んでいないことが確認された製品

次の製品は、このアドバイザリに記載されている脆弱性の影響を受けません。

- Cisco TelePresence EC20
- Cisco Telepresence Touchデバイス

IOS、IOS-XE、IOS-XR、およびNX-OSベースのシスコ製品はlibupnpを使用しないため、この脆弱性の影響を受けません。

Cisco ASAシリーズ適応型セキュリティアプライアンス(ASA)およびファイアウォールサービスモジュール(FWSM)はlibupnpを使用しないため、この脆弱性の影響を受けません。

このセクションは、より詳細な情報が入手可能になると更新されます。

詳細

UPnP™は、オペレーティングシステム、プログラミング言語、または物理ネットワーク接続に関係なく、ネットワーク上のデバイスの検出、イベント通知、および制御を可能にするアーキテクチャです。UPnP™は、TCP/IP、HTTP、XMLなどの一般的なインターネット規格と仕様に基づいています。

Portable SDK for UPnP Devicesは、リモートで利用可能な少なくとも3つのバッファオーバーフローの影響を受けます。これらの脆弱性は、UDPポート1900での着信SSDP要求の処理で不正利用される可能性があります。CERTは、これらの脆弱性を文書化するために次のCVE IDをリリースしました：CVE-2012-5958、CVE-2012-5959、CVE-2012-5960、CVE-2012-5961、CVE-2012-5962、CVE CVE-2012-5964およびCVE-2012-5965

次のCisco Bug IDは、UPnPの問題が発生する可能性を追跡するために使用されています。次に示すバグは、製品に脆弱性が存在することを確認するものではなく、製品が適切な製品チームによって調査中であることを確認するものです。

シスコの登録ユーザは、Cisco Bug Toolkit(http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl)でこれらのバグを確認できます。

製品	Bug ID
Cisco AP541N ワイヤレス アクセス ポイント	0.CSCue19294
Cisco NSS300シリーズスマートストレージ**	0.CSCue19395
Cisco PVC2300ビジネスインターネットビデオカメラ**	0.CSCue21009
Cisco RV0XXシリーズルータ**	0.CSCue20980
Cisco RV220Wワイヤレスネットワークセキュリティファイアウォール	0.CSCue20983
Cisco RV120W Wireless-N VPNファイアウォール	0.CSCue20983
Cisco RVL200 VPNルータ**	0.CSCue20989
Cisco RVS4000ギガビットセキュリティルータ**	0.CSCue20997
Cisco Small Business ISA500 Series Integrated Security Appliances	0.CSCue19341
Cisco Small Business SA500 シリーズ セキュリティ アプライアンス	0.CSCue21031
Cisco TelePresence Cシリーズエンドポイント	0.CSCue19318
Cisco TelePresence System EX シリーズ	0.CSCue19318
Cisco TelePresence SX20	0.CSCue19318
Cisco WAP4400N Wireless-Nアクセスポイント	0.CSCue21567
Cisco WET200 Wireless-Gビジネスイーサネットブリッジ	0.CSCue21572
Cisco WRVS4400N Wireless-Nギガビットセキュリティルータ**	0.CSCue21578
Cisco WRV200 Wireless-G VPNルータ**	0.CSCue21578

**注：この製品は販売されておらず、サポートされていない可能性があります。

NSS3000サポート終了通知については、
http://www.cisco.com/en/US/prod/collateral/ps4159/ps9954/ps9957/end_of_life_c51_606545.htmlを参照してください。

PVC2300サポート終了通知については、
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9692/ps9944/end_of_life_notice_c51-685005.htmlを参照してください。

RVシリーズルータのサポート終了通知については、
http://www.cisco.com/en/US/products/ps9923/prod_eol_notices_list.htmlを参照してください。

回避策

UPnPは、Webユーザインターフェイスを使用して多くのデバイスで無効にすることができます

。UPnPを無効にする手順については、通常は『 Product Administration Guide』を参照してください。たとえば、『 RV-120Wアドミニストレーションガイド』の「ファイアウォールの基本設定」セクションには、UPnPを有効/無効にするチェックボックスがあります。詳細については、http://www.cisco.com/en/US/docs/routers/csbr/rv110w/administration/guide/rv110w_admin.pdf#page84を参照してください。

お客様は、ワイヤレスデバイスを設定する際に、「ゲスト」アクセスを許可しない、ログインに認証資格情報を要求するなど、基本的な強化ルールに従う必要があります。

また、インフラストラクチャアクセスコントロールリスト(iACL)を使用して、UDPポート1900の信頼できないホストから該当するデバイスへのトラフィックをブロックすることもできます。この保護メカニズムにより、これらの脆弱性を悪用しようとするパケットがフィルタリングされて廃棄されます。

また、Cisco ASA 5500シリーズ適応型セキュリティアプライアンス、Cisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用のFirewall Services Module(FWSM)でも、トランジットアクセスコントロールリスト(tACL)を使用して、脆弱性の悪用を効果的に防止できます。

シスコは、これらの脆弱性が悪用される可能性を検出して緩和する方法を説明したApplied Mitigation Bulletin(AMB)をリリースしています。AMBは、https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=28005から入手できます。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の可能性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デバイス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規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

この問題はCERT-CCによって調整され、公開されました。これらの脆弱性に関する注は、http://www.kb.cert.org/vuls/id/922681で参照できます。

この脆弱性はHD Mooreによって発見され、JP-CERTおよびUS-CERTによってシスコに報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130129-upnp

改訂履歴

リビジョン 1.2	2013年2月13日	「該当製品」リストに「確認済み製品」を追加し、RVシリーズルータの販売終了とサポート終了に関する通知を追加。
リビジョン 1.1	2013年1月30日	「Cisco適用対応策速報」へのリンクを追加。
リビジョン 1.0	2013年1月29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。