UPnP デバイスのための携帯用 SDK はバッファオーバーフローの脆弱性が含まれています

Critical

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 Plug-n-Play （ UPnP ）デバイスのための携帯用ソフトウェア開発者キット（ SDK ）は最初に悪意のある簡単なサービスを複数のスタックベース バッファオーバーフローに脆弱 Discovery Protocol （ CDP ）処理するとき（ SSDP ）要求するである UPnP デバイスのための Intel SDK として知られている libupnp ライブラリが、含まれています。 このライブラリはメディア ストリーミングおよびファイル 共有 アプリケーションに加えて複数のベンダー 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 CERT 脆弱性に関する注記のに、 http://www.kb.cert.org/vuls/id/922681 で表示することができる VU#922681 表われました。

Cisco は現在これらの脆弱性への可能性のある公開のための製品を評価しています。 このアドバイザリは、次のリンクより確認できます。
129-upnp

該当製品

Cisco は現在 UPnP これらの脆弱性への可能性のある公開のための製品を評価しています。 製品はこのアドバイザリの「脆弱性が存在する製品」または「脆弱性が存在しない製品」セクションに製品公開についての最終的な判断がなされる場合だけリストされます。 これら二つのセクションのにリストされていない製品はまだ評価されています。

脆弱性のある製品

以下の製品はこのアドバイザリに説明がある脆弱性から影響を受けます:

- 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

このセクションは時更新済です。

脆弱性を含んでいないことが確認された製品

以下の製品はこのアドバイザリに説明がある脆弱性から影響を受けません:

- Cisco TelePresence EC20
- Cisco TelePresence Touch デバイス

IOS、IOS、IOS XR および NX-OS に基づくシスコ製品は libupnp を使用しないし、影響を受けていません。

Cisco ASA シリーズ 適応型セキュリティ アプライアンス（ASA）ソフトウェアおよびファイアウォールサービス モジュール（FWSM）は libupnp を使用しないし、影響を受けていません。

このセクションは時更新済です。

詳細

UPnP™はネットワークのデバイス、オペレーティング システムの依存しない、プログラミング言語、または物理的 な ネットワーク接続の検出、イベント 通知および制御を有効に する アーキテクチャです。 UPnP™は TCP/IP、HTTP および XML のようなよくあるインターネット規定および仕様に基づいています。

UPnP デバイスのための携帯用 SDK は少なくとも 3 つのリモートで開発可能なバッファオーバーフローから影響を受けます。 これらの脆弱性は UDP ポート 1900 の着信 SSDP 要求の処理で不正利用することができます。 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-2012-5963、CVE-2012-5964 および CVE-2012-5965。

次の Cisco バグ ID が UPnP 問題への潜在的な公開をトラッキングするのに使用されています。バグは製品が適切な製品チームによって調査中であること製品が脆弱であるが、むしろことを下記に確認しませんリストしました。

登録済みの Ciscoカスタマーは Ciscoバグ ツールキットによってこれらのバグを表示できます: http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl

Product	Bug ID

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

** この製品は現在は販売されていなくて、サポートされないかもしれません。

http://www.cisco.com/en/US/prod/collateral/ps4159/ps9954/ps9957/end_of_life_c51_606545.html で NSS3000 廃止表記を表示して下さい。

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9692/ps9944/end_of_life_notice_c51-685005.html で PVC2300 廃止表記を表示して下さい。

http://www.cisco.com/en/US/products/ps9923/prod_eol_notices_list.html で RV シリーズ ルータ 廃止表記を表示して下さい

回避策

UPnP は Web ユーザ ユーザー・ インターフェースを使用して多くのデバイスでディセーブルにすることができます。 方法に関する手順は *製品管理 ガイド*で UPnP をディセーブルにする一般に与えられます。 たとえば、 *RV-120W 管理 ガイド*の「基本的なファイアウォール設定」セクションで行います、UPnP を有効または無効にするチェックボックスがあります。 その他の情報に関しては、
http://www.cisco.com/en/US/docs/routers/csbr/rv110w/administration/guide/rv110w_admin.pdf#page84 を参照して下さい。

顧客は「ゲスト」アクセスを許可しないことおよび認証クレデンシャルをログインするように要求することのようなワイヤレス デバイスを、設定した場合ルールを堅くする基本に続く必要があります。

顧客はまたインフラストラクチャ アクセスコントロール アクセス・ コントロール・ リスト

（iACLs）を使用して UDP ポート 1900 の信頼できないホストから影響を受けたデバイスにトラフィックをブロックできます。 この保護メカニズムはこれらの脆弱性を不正利用するように試みているパケットをフィルタリングし、廃棄します。

有効なエクスプロイト防止はまた Cisco ASA 5500 シリーズによって中継アクセスコントロールアクセス・コントロール・リスト（tACLs）を使用している Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータにおよび Firewall Services Module （FWSM）適応型セキュリティ アプライアンス（ASA）ソフトウェア提供することができます。

Cisco はこれらの脆弱性の潜在的な不正利用を検出する軽減する方法を説明する応用軽減情報（AMB）を発表しました。 AMB は利用できますで: http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=28005

修正済みソフトウェア

ソフトウェアアップグレードを検討するとき、顧客は Cisco Security Advisory、応答および表記アーカイブを http://www.cisco.com/go/psirt で参照し、公開および完全なアップグレード ソリューションを判別するためにそれに続くアドバイザリを検討するように勧告されます。

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。

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、表われました。 脆弱性に関する注記は http://www.kb.cert.org/vuls/id/922681 で表示することができます。

この脆弱性は HD ムーアによって検出され、Cisco に JP-CERT および US-CERT によって報告されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130129-upnp

改訂履歴

リビジョン 1.2	2013-February-13	RV シリーズ ルータのための影響を受けたリストおよび追加された EOS/EOL 表記への追加された確認された製品。
リビジョン	2013-January-30	Cisco によって加えられた軽減情報にリンクを追加しました。

1.1		
リビジョン 1.0	2013-January-29	初回公開リリース

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。