多重シスコ製品 libSRTP サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20160420-libsrtp

初公開日 : 2016-04-20 16:00

最終更新日 : 2016-05-10 17:14

バージョン 1.1 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCux35568 CSCux01782 CSCux04317 CSCux00742 CSCux00686 CSCux00697 CSCux01786 CSCux00711 CSCux00745 CSCux00748 CSCux00716 CSCux00708 CSCux00707 CSCux00729 CSCux37802

CVE-2015-6360

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

サービス拒否（DoS）脆弱性に対処するセキュア Real-Time Transport Protocol（RTP）（SRTP）ライブラリの Cisco リリースバージョン 1.5.3（libSRTP）。 複数のシスコ製品は libSRTP ライブラリの脆弱なバージョンを織込んでいます。

脆弱性は libSRTP の暗号化処理サブシステムにあり、リモート攻撃者非認証が DoS 状態を誘発するようにする可能性があります。 脆弱性は SRTP パケットのある特定のフィールドの不適当な入力の検証が原因です。 攻撃者は設計されている巧妙に細工された SRTP パケットの送信によって影響を受けたデバイスに問題を誘発するようにこの脆弱性を不正利用する可能性があります。

この脆弱性 on Cisco 製品の影響は影響を受けた製品によって変わるかもしれません。 各製品の影響についての詳細はで「調節します」この脆弱性のための各 Ciscoバグのセクションを概説されます。 バグID はこの状況報告のおよび「脆弱性が存在する製品の表の上でリストされています」。

このアドバイザリは、次のリンクより確認できます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-libsrtp

該当製品

脆弱性のある製品

以下のシスコ製品はこの脆弱性によって影響を与えられるために確認されました:

Product	Defect	Fixed Release Availability
Collaboration and Social Media		
Cisco WebEx Meetings Server versions 1.x	CSCux00729	
Cisco WebEx Meetings Server versions 2.x	CSCux00729	2.6.1 および 2.7 （6月 2016）
Endpoint Clients and Client Software		
Cisco Jabber Guest	CSCuz52891	
Cisco Jabber for Android	CSCuz52906	11.6
Apple iOS のための Cisco Jabber	CSCux82920	11.6
Cisco Jabber for Mac	CSCuz52915	11.6
Cisco Jabber for Windows	CSCux80499	11.6
Network and Content Security Devices		
Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア[1]	CSCux00686	8.4.7.31 9.1.7 9.2.4.6 9.3.3.8
Routing and Switching - Enterprise and Service Provider		
Cisco IOS XE ソフトウェア[2]	CSCux04317	3.14.3S 3.13.5S 3.16.2S 3.10.7S 3.17.1S 3.15.3S
Voice and Unified Communications Devices		
Cisco IP Phone 88x1 シリーズ	CSCux00708	11.0(1)
Cisco DX シリーズ IP フォン	CSCux00697	10.2(5)
Cisco IP Phone 88x5 シリーズ	CSCux00748	11.0(1)
Cisco Unified 7800 Series IP Phones	CSCux00742	11.0(1)
Cisco Unified 8831 シリーズ IP Conference Phone	CSCux01782	
Cisco Unified 8961 IP フォン	CSCux00707	9.4(2)SR3 （August 2016）
Cisco Unified 9951 IP フォン	CSCux00707	9.4(2)SR3 （August 2016）
Cisco Unified 9971 IP フォン	CSCux00707	9.4(2)SR3 （August 2016）
Cisco Unified Communications Manager（UCM）	CSCux00716	10.5(2)SU3
Cisco Unified Communications Manager Session Management Edition（SME）	CSCux00716	10.5(2)SU3
Cisco Unified Communications for Microsoft Lync	CSCuz52971	11.6 （2016）夏
Cisco Unified IP Phone 7900 Series	CSCux00745	9.4(2)SR2
Cisco Unified IP Phone 8941 および 8945 （SIP）	CSCux01786	
Cisco Unified Wireless IP Phone	CSCux37802	1.4.8.4
Cisco Unity Connection（UC）	CSCux35568	10.5(2)SU3
Cisco Virtualization Experience Media Engine	CSCuz52961	11.7 （9月 2016）

1. Cisco ASA はリリース 9.4.1 現在で SRTP を使用する電話プロキシ機能を非難しました。

2. Cisco IOS XE プラットフォームは Cisco Unified Border Element （キューブ）またはセッション ボーダー コントローラ（SBC）機能を SRTP セッションを終了するか、または変換すればのに使用するように設定される場合脆弱です。

脆弱性を含んでいないことが確認された製品

多くのシスコ製品は、Cisco IOSソフトウェアのような、サポート SRTP しかし libSRTP を使用しません。 従って、それらはこの脆弱性から影響を受けません。 Cisco IOS XR ソフトウェアおよび Cisco NX-OS ソフトウェアは libSRTP を使用しません。 製品はこの脆弱性からこの状況報告の「脆弱性が存在する製品」セクションにリストされていなければ影響を受けません。

詳細

libSRTP ライブラリは最初に Cisco 社によって書かれ、 https://github.com/cisco/libsrtp でダウンロードのために利用可能な SRTP のオープンソース実装です。 脆弱性は共用利用可能ソースコードにあり、従って libSRTP のリリース以来のライブラリは 1.5.3 前にすべてのバージョンに影響を与え。 問題は sanitization を入力すること不十分によって SRTP パケットである特定のフィールドを処理するとき引き起こされています。 問題を誘発するように設計されているパケットを処理するによりそれに続くメモリ オペレーションの失敗という結果に終る可能性がある整数アンダーフローを引き起こすかもしれません。 このアンダーフローが行われる場合、パケットの復号化は可能性がありま、メモリ不良失敗する、アプリケーション クラッシュ、またはシステム 再始動を引き起こします。 この脆弱性 on Cisco 製品の影響は影響を受けた製品によって変わります。

回避策

回避策は今後 Cisco bugs に記載され、 Cisco Bug Search Tool を使用して検索可能です。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

また、お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定リセラーまたはパートナーからそのソフトウェアの有効なライセンスを取得している場合に限り

ます。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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 Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

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は確認していません。

出典

Cisco はこの脆弱性を検出し、報告するために Mozilla チームとの Randell Jesup に感謝することを望みます。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-libsrtp

改訂履歴

Version	Description	Section	Status	日付
1.1	更新済修正済み バージョン表。	脆弱性のある製品	Final	2016-May-10
1.0	初回公開リリース		Final	2016-April-20

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。