

Cisco Jabber STARTTLSダウングレードの脆弱性

Medium

アドバイザリーID : cisco-sa-20151224-jab

[CVE-2015-6409](#)

初公開日 : 2015-12-24 18:30

最終更新日 : 2016-02-03 21:33

バージョン 2.1 : Final

CVSSスコア : [4.3](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCux80122](#)

[CSCux74900](#) [CSCux88529](#)

[CSCux74895](#) [CSCux74848](#)

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 Jabberクライアントの脆弱性により、認証されていないリモートの攻撃者がSTARTTLSダウングレード攻撃を実行する可能性があります。

この脆弱性は、クライアントがTransport Layer Security(TLS)を使用してExtensible Messaging and Presence Protocol(XMPP)接続が確立されていることを確認しないことに起因します。攻撃者は、中間者攻撃を実行してXMPP接続を改ざんし、TLSネゴシエーションを回避することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はクライアントにクリアテキストXMPP接続を確立させる可能性があります。

シスコでは、この脆弱性に対処するソフトウェア アップデートをリリースする予定です。この脆弱性に対処する回避策はありません。

このアドバイザリーは次のリンクで確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151224-jab>

該当製品

脆弱性のある製品

次の表に、本アドバイザリに記載された脆弱性の影響を受けるシスコ製品を示します。

製品	Defect	Fixed Release Availability
クライアント側		
Cisco Jabber for Windows	CSCux88529	11.5(1)オンプレミス (利用可能)
		11.5(1)クラウド (2016年2月4日)
		11.1(3)オンプレミス (2016年2月5日)
		11.1(3)クラウド (2016年2月18日)
		10.6(7)オンプレミス (2016年2月12日)
		10.6(7)クラウド (2016年2月25日)
		10.5(5) (2016年2月18日 – 仮称)
Cisco Jabber for Mac	CSCux74900	9.7(7) (2016年2月23日 – 仮称)
		11.5(1)オンプレミス (2016年2月3日)
Cisco Jabber for Android	CSCux74895	11.5(1)クラウド (2016年2月4日)
		11.5(1) (入手可能)
Cisco Jabber for iPhone and iPad	CSCux74848	11.5(1) (2016年2月5日 – 仮称)
サーバ側		
Cisco Unified Communications Manager IM & Presence Service	CSCux80122	COPファイル (利用可能)

このアドバイザリが最初に公開された時点では、リリース11.5(0)を含む、影響を受ける製品のすべてのリリースに脆弱性が存在していました。

脆弱性を含んでいないことが確認された製品

該当するJabberクライアントの音声およびビデオテレフォニー機能の動作はXMPPプロトコルに依存しないため、この脆弱性の影響を受けません。

次の製品は、この脆弱性の影響を受けません。

- Cisco Jabber Video for iPad
- Cisco Jabber Voice for iPhone
- Cisco Jabber Voice for Android
- Cisco UC Integration for Microsoft Lync
- Cisco Jabber Guest
- Cisco Jabber Software Development Kit

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

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

このアドバイザリの「脆弱性が存在する製品」セクションの表を参照して、修正プログラムの入手可能性に関する情報を確認してください。

また、オンプレミスの導入では、保護をオンプレミスクライアントに拡張するために、Cisco Unified Communications Manager IM & Presenceサービスのアップデートも必要になります。

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。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) は、アドバイザリで説明されている脆弱性に対して概念実証段階のエクスプロイト コードが入手可能であることを認識しています。Cisco PSIRTでは、この脆弱性が悪用された事例は確認されていません。

出典

シスコは、この脆弱性を発見し、報告していただいたSynacktiv社のRenaud Dubourgais氏およびSébastien Dudek氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151224-jab>

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.1	修正済みリリースの入手可能性に関する情報を更新。	Affected Products - Vulnerable Products	Final	2016年2月

				3 日
2. 0	脆弱性に対処するコード変更は、11.5(0)リリース直前に不具合 CSCuw87419から削除されました。これは、CUCM IM&Pビルドを使用する展開で限定的な暗号化機能を使用する場合にオンプレミスの接続の問題が発生するためです。該当する不具合はすべて新しいプラットフォームで公開されており、この脆弱性の適切なアドレッシングを追跡しています。	該当製品 – 脆弱性が存在する製品、該当製品 – 脆弱性が存在しないことを確認した製品、修正済みソフトウェア	Fi n al	20 16 年 1月 18 日
1. 3	脆弱な製品のリストにCisco Jabber for Macを追加。Cisco Jabber Voice for iPhone、Cisco Jabber Video for iPad、およびCisco Jabber Voice for Androidを、脆弱性が存在しない製品のリストに移動しました。概念実証のエクспロイトコードが利用可能になったことを示します。	該当製品 – 脆弱性が存在する製品、該当製品 – 脆弱性が存在しないことを確認した製品、不正利用事例、公式発表	Fi n al	20 16 年 1月 8日
1. 2	すべてのプラットフォームのリリース11.5に修正が含まれ、クライアントの異なるモバイルバージョンに明示的に名前が付けられ、脆弱性のあるバージョンが修正されて11.5を除くすべてのリリースが含まれるようになりました。	該当製品 – 脆弱性が存在する製品、修正済みソフトウェア	Fi n al	20 16 年 1月 5 日
1. 1	Cisco Jabber for iPhoneおよびiPadとCisco Jabber for Androidの該当バージョンを含むように更新されました。	タイトル、サマリー、影響を受ける製品 – 脆弱性のある製品	Fi n al	20 16 年 1月 4 日
1. 0	初回公開リリース	-	Fi n al	20 15 年 12月 24 日

利用規約

本アドバイザー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。本アドバイザー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。

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