Cisco Unified Presence and Jabber Extensible Communications Platform Stream Header Denial of Service Vulnerability

Advisory ID: cisco-sa-20120912-cupxcp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120912-cupxcp

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。

Revision 1.0

For Public Release 2012 September 12 16:00 UTC (GMT)

目次

要約

Cisco Unified Presence および Jabber Extensible Communications Platform（Jabber XCP）には、DoS（サービス拒否）の脆弱性が存在します。認証されていないリモートの攻撃者が、巧妙に細工された Extensible Messaging and Presence Protocol（XMPP）ストリーム ヘッダを該当サーバに送信することで、この脆弱性を不正利用できる可能性があります。この脆弱性が悪用されると、Connection Manager プロセスのクラッシュが引き起こされる可能性があります。この脆弱性が繰り返し悪用されると、継続的な DoS 状態となる可能性があります。

この脆弱性の不正利用を軽減する回避策はありません。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。このアドバイザリは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120912-cupxcp

該当製品

脆弱性が存在する製品

次に示したバージョンの Cisco Unified Presence および Jabber Extensible Communications Platform（Jabber XCP）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。脆弱性のあるバージョンの Jabber XCP ソフトウェアを実行している JabberNow アプライアンスも影響を受けます。

Cisco Unified Presence

Cisco Unified Presence の 8.6(3) より前のすべてのバージョンが、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。

Jabber XCP および JabberNow アプライアンス

Jabber XCP ソフトウェアの 5.3 より前のすべてのバージョンが、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 Unified Presence ソフトウェア バージョンの確認

Cisco Unified Presence ソフトウェアのバージョンを判断するには、コマンド ライン インターフェイスで **show version active** コマンドを発行します。

次の例は、Cisco Unified Presence ソフトウェア バージョン 8.6.0 を示しています。

```
admin: show version active
Active Master Version: 8.6.0.97041-43
```

Jabber XCP ソフトウェア バージョンの確認

Jabber XCP ソフトウェアのバージョンを判断するには、[JABBER_HOME]/var/cache/xcp_vars.sh ファイルから **JABBER_VERSION** を見付けます。

次の例は、Jabber XCP ソフトウェア バージョン 5.8.1.17421 を示しています。

```
$ cat [JABBER_HOME]/var/cache/xcp_var.sh | grep JABBER_VERSION
JABBER_VERSION=5.8.1.17421
```

脆弱性が存在しない製品

他のシスコ製品において、この脆弱性の影響を受けるものは現在確認されていません。

詳細

Cisco Unified Presence および Jabber XCP は、オープンで拡張性のあるプラットフォームを提供することにより、アベイラビリティおよびインスタント メッセージング（IM）情報の安全な交換を促進します。

Cisco Unified Presence には、認証されていないリモートの攻撃者が DoS 状態を引き起こす可能性のある脆弱性が含まれます。

JabberNow アプライアンスを含む Jabber Extensible Communications Platform には、認証されていないリモートの攻撃者が DoS 状態を引き起こす可能性のある脆弱性が含まれます。

XMPP クライアントは、IP バージョン 4（IPv4）または IP バージョン 6（IPv6）を使用してストリーム ヘッダを送信することで、XMPP サーバと通信を開始します。この脆弱性は、ストリーム ヘッダの誤った処理に起因します。攻撃者は巧妙に細工された XMPP ストリーム ヘッダを該当システムに送信することで、この脆弱性を不正利用できる可能性があります。不正利用に成功した場合、Connection Manager プロセスが終了され、既存のクライアントの接続が切断されると共に、新たなクライアントが接続できなくなる可能性があります。Connection Manager プロセスは自動的に再起動されます。しかし、繰り返し悪用されると、継続的な DoS 状態となる可能性があります。

XMPP ストリーム ヘッダの詳細については、RFC 6120 より入手可能です。

この脆弱性は、Cisco Bug ID CSCtu32832（ 登録ユーザのみ ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2012-3935 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCtu32832 - CUP and Jabber XCP Stream Header Denial of Service Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.1**		
Exploitability	Remediation Level	Report Confidence
Proof-of-Concept	Official-Fix	Confirmed

影響

この脆弱性の不正利用に成功した場合、Connection Manager プロセスが終了され、既存のクライアントの接続が切断されると共に、新たなクライアントが接続できなくなる可能性があります。Connection Manager プロセスは自動的に再起動されます。しかし、この脆弱性が繰り返し悪用されると、該当サーバのすべてのユーザに対して継続的な DoS 状態が引き起こされる可能性があります。

ソフトウェア バージョンおよび修正

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、本アドバイザリ以降に公開のアドバイザリを参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が不明確な場合は、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。

Cisco Unified Presence Software Version	First Fixed Release
All versions prior to 8.6(3)	Upgrade to 8.6(3) or higher

Jabber XCP Software Version, Including JabberNow Appliances	First Fixed Release
All versions prior to 5.3	Upgrade to 5.3 or higher

回避策

この脆弱性を軽減する回避策はありません。

ネットワーク内のシスコ デバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Intelligence』にて参照できます。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=26732

修正済みソフトウェアの入手

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。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

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、ご購入いただいたフィーチャ 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、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレードを入手することができます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、適切な処置について支援を受けてください。

回避策の効果は、使用製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策または修正が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

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。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このアドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC を通して無償アップグレードをお求めください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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不正利用事例とその公表は確認しておりません。

本アドバイザリで説明した脆弱性は、シスコ内部でのテストによって発見されました。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120912-cupxcp

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

このアドバイザリに関する今後の更新があれば、Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.0	2012-September-12	Initial public release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスして

ください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。