Cisco Security Advisory: Jabber Extensible Communications Platform and Cisco Unified Presence XML Denial of Service Vulnerability

Advisory ID: cisco-sa-20110928-xcpcupsxml

http://www.cisco.com/warp/public/707/cisco-sa-20110928-xcpcupsxml.shtml

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 2011 September 28 1600 UTC (GMT)

目次

要約

Jabber Extensible Communications Platform（Jabber XCP）および Cisco Unified Presence には、サービス拒否（DoS）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、悪意のある XML を該当サーバに送信することで、この脆弱性を不正利用する可能性があります。この脆弱性の不正利用に成功した場合、メモリおよび CPU の負荷が非常に大きくなり、その結果、メモリの枯渇や処理のクラッシュが発生す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。

このアドバイザリは次のリンクに掲載されます。 http://www.cisco.com/warp/public/707/cisco-sa-

20110928-xcpcupsxml.shtml

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 8.5(4) 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

次に示したバージョンの Jabber XCP ソフトウェアは、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。

Versions	Builds
2.X	All builds
3.X	All builds
4.X	All builds
5.0	All builds
5.1	All builds
5.2	All builds
5.4	Prior to 5.4.0.27581
5.8	Prior to 5.8.1.27561

注：これらのソフトウェア バージョンを実行している JabberNow アプライアンスも、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_VERSION** を *[JABBER_HOME]/var/cache/xcp_vars.sh* ファイルから探します。

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。

```
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。

詳細

Jabber XCP および Cisco Unified Presence 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。

Jabber XCP（JabberNow アプライアンスを含む）および Cisco Unified Presence の XML パーサーには、Exponential Entity Expansion 攻撃に対する脆弱性があります。この攻撃は、*XML 爆弾*とも呼ばれます。 これは、XML スキーマのルール上は有効でも、パーサーまたは基盤のサーバをハングまたはクラッシュさせる XML ドキュメントです。XML パーサーが文字列の *lol* または *ha* をサーバ リソースが枯渇するまで繰り返すことが、多数の概念実証によって判明しています。このことから、この攻撃は *Billion Laughs Attack* と呼ばれる場合もあります。

この攻撃では、XML の特定のプロパティを組み合わせ、最高レベルの入れ子置換を使用して、有効でありながら悪意のある XML を作成します。XML パーサーが、入れ子になったすべてのエンティティを拡張しようとすると、すぐにサーバのリソースはすべて枯渇してしまいます。

このテクニックは、Cisco Unified Presence および Jabber XCP（JabberNow アプライアンスを含む）の XML パーサーにより、CPU およびメモリの使用率を上昇させ、処理をクラッシュさせます。クライアント/サーバ接続だけでなく、サーバ/サーバ（フェデレーション）リンクも影響を受けます。

この脆弱性は、次の Cisco Bug ID で文書化されています。

- CSCtq78106（ 登録ユーザのみ ）
- CSCtq89842（ 登録ユーザのみ ）
- CSCtq88547（ 登録ユーザのみ ）

この脆弱性に対して、Cisco Bug ID CSCtq78106 には Common Vulnerabilities and Exposures（CVE）ID CVE-2011-3287、Cisco Bug ID CSCtq89842 および CSCtq88547 には CVE ID CVE-2011-3288 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、個々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 URL にて CVSS に関する FAQ 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 計算ツールを以下の URL にて提供しています。

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

CSCtq78106 - XCP Vulnerable to XML Entity Expansion Attack **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 - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtq89842 - CUP Server PE Vulnerable to XML Entity Expansion Attack **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 - **6.4**					

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCtq88547 - CUP Server Client Profile Agent Vulnerable to XML Entity Expansion Attack 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 - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用に成功した場合、メモリおよび CPU の負荷が非常に大きくなり、その結果、メモリの枯渇や処理のクラッシュが発生す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。

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際には、 http://www.cisco.com/go/psirt/ および本アドバイザリ以降に公開のアドバイザリも参照して、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 8.5(4)	Upgrade to 8.5(4)

Jabber XCP Software	**First Fixed Release**

Version, Including JabberNow Appliances	
Versions prior to 4.X	These versions are vulnerable but are End of Life.No fixed software will be made available.Cisco highly recommends that customers using one of these versions migrate to a supported version.
Versions 4.X - 5.2	Migrate to 5.4.0.27581, 5.8.1.27561, or higher
Version 5.4	Upgrade to 5.4.0.27581, 5.8.1.27561, or higher
Version 5.8	Upgrade to 5.8.1.27561 or higher

回避策

この脆弱性を軽減する回避策はありません。

修正済みソフトウェアの入手

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。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 ライセンスの条項または、Cisco.com Downloads の http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他の条項に従うことに同意したことになります。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

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、シスコのワールドワイド Web サイト上の Software Center 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

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、本脆弱性に関する適切な処置について指示と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。TAC の連絡先は次のとおりです。

- +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、このお知らせの 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に対する無償アップグレードは、TAC 経由でご要求いただく必要があります。

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、 http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html を参照してください。

不正利用事例と公式発表

XML エンティティ拡張攻撃はよく知られていますが、Cisco PSIRT では、本アドバイザリに記載されているシスコ製品の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。

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

本アドバイザリは、次のシスコのワールドワイド Web サイト上に掲載されます。

http://www.cisco.com/warp/public/707/cisco-sa-20110928-xcpcupsxml.shtml

ワールドワイド Web 以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- 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
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものもシスコのワールドワイド Web サイトに掲載される予定です。 しかしながら、前述のメーリング リストもしくはニュースグループに対し 積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最新情報を ご確認いただくことをお勧めいたします。

更新履歴

Revision 1.0	2011-September-28	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、シスコ ワールドワイド Web サイトの

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。このページには、シスコのセキュリティ通知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。