Cisco Unified PresenceおよびJabber Extensible Communications Platformのストリームヘッダーにおけ るDoS脆弱性

アドバイザリーID : cisco-sa-20120912-cupxcp
初公開日 : 2012-09-12 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCtu32832

CVE-2012-3935

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 Unified PresenceおよびJabber Extensible Communications Platform(Jabber XCP)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、巧妙に細工されたExtensible Messaging and Presence Protocol(XMPP)ストリームヘッダー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すると、接続マネージャプロセスがクラッシュ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、DoS 状態が続く可能性があります。

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ソフトウェアアップデートをリリースしています。 このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120912-cupxcp

該当製品

脆弱性のある製品

次のバージョンの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

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

Jabber XCPおよびJabberNowアプライアンス

5.3より前のすべてのバージョンの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。

Cisco Unified Presenceソフトウェアバージョンの確認

実行中のCisco Unified Presenceソフトウェアのバージョンを確認するには、コマンドラインインターフェイスから 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ソフトウェアの実行バージョンを確認するには、[JABBER_HOME]/var/cache/xcp_vars.shファイルで JABBER_VERSIONを検索します。

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。

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

脆弱性を含んでいないことが確認された製品

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

Cisco Unified PresenceとJabber XCPは、オープンで拡張性の高いプラットフォームを提供し、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

のある脆弱性が存在します。

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存在します。

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ーを送信することで、XMPPサーバとの通信を開始します。この脆弱性は、ストリームヘッダーの不適切な処理に起因します。攻撃者は、巧妙に細工されたXMPPストリームヘッダー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する可能性があります。エクスプロイトに成功すると、接続マネージャプロセスが終了し、既存のクライアントの接続がドロップされて新しいクライアントの接続が妨げられる可能性があります。接続マネージャプロセスが自動的に再起動します。ただし、繰り返し悪用されると、持続的なDoS状態が発生する可能性があります。

XMPPストリームヘッダーの詳細については、RFC 6120を参照してください。

この脆弱性は、Cisco Bug ID CSCtu32832(登録ユーザ専用)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。

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 Cisco デバイスに導入できる追加の緩和策については、このアドバイザリに関連する Cisco 適用インテリジェンス（ https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=26732 ）を参照してください。

修正済みソフトウェア

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。

Cisco Unified Presenceソフトウェアバージョン	First Fixed Release（修正された最初のリリース）

8.6(3)より前のすべてのバージョン	8.6(3)以降にアップグレード

Jabber XCPソフトウェアバージョン（JabberNowアプライアンスを含む）	First Fixed Release（修正された最初のリリース）
5.3より前のすべてのバージョン	5.3以降にアップグレード

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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やその公表を確認していません。

このアドバイザリで説明されている脆弱性は、シスコの社内テストで発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120912-cupxcp

改訂履歴

リビジョン 1.0	2012年9月12日	初版リリース

利用規約

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。