Cisco Contact Centerソリューションにおける Apache Log4jの脆弱性の影響について

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[ICMサーバでのTomcatバージョンの確認](#)
[よくある質問](#)

概要

このドキュメントでは、Apache Log4jの脆弱性がCisco Contact Center(UCCE)製品ラインに及ぼす影響について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Unified Contact Center製品バージョン11.6以降

背景説明

Apacheは最近、Log4jコンポーネントの脆弱性を発表しました。これはCisco Contact Centerソリューションで広く使用されており、シスコは製品ラインナップの評価を積極的に行い、安全性と影響を確認しています。

> **注：** 詳細については、次のサイトを参照してください。[シスコセキュリティアドバイザリ – cisco-sa-apache-log4j]

このドキュメントでは、情報が利用可能になった時点でさらに詳細な情報を提供します（図15を参照）。

ID	11.6.2	12.0(1)	12.5(1)	12.6(1)

UCCE/ICM	CSCwa47273	パッチ – 11.6(2)_ES84 ReadMe	パッチ – 12.0(1)_ES91 ReadMe	パッチ – 12.5(1)_ES101 ReadMe *注 1：ES_55パッチが必要です。OpenJDK Migrationドキュメントを参照してください* *注 2：Tomcatバージョンの確認：下記の「ICMサーバでのTomcatバージョンの確認」の項を参照してください*	パッチ – 12.6(1)_ES1 ReadMe
PCCE	CSCwa47274	パッチ – 11.6(2)_ES84 ReadMe	パッチ – 12.0(1)_ES91 ReadMe	パッチ – 12.5(1)_ES101 ReadMe *注 1：ES_55パッチが必要です。OpenJDK Migrationドキュメントを参照してください* *注 2：Tomcatバージョンの確認：下記の「ICMサーバでのTomcatバージョンの確認」の項を参照してください*	パッチ – 12.6(1)_ES1 ReadMe
CTIOS		影響なし	影響なし	影響なし	影響なし
	ID	**11.6(1)**	**12.0(1)**	**12.5(1)**	**12.6(1)**
CVP	CSCwa47275	パッチ – 11.6(1) ES16 Readme	パッチ – 12.0(1)_ES10 ReadMe	パッチ – 12.5(1)_ES25 ReadMe	パッチ – 12.6(1)_E ReadMe
VVB	CSCwa47397	影響なし	影響なし	パッチ – 12.5(1)_ES12 Readme	パッチ – 12.6(1)_E ReadMe ** use patch published o 2021 12月2*
Call Studio	CSCwa54008	Callstudio_11.6_Log4j_fix ReadMe	Callstudio_12.0(1)_Log4j_fix ReadMe	Callstudio_12.5(1)_Log4j_fix ReadMe	Callstudio_1)_Log4j_fix ReadMe
Finesse	CSCwa46459	影響なし	影響なし	影響なし	パッチ – 12.6(1)_E ReadMe
CUIC	CSCwa46525	影響なし	影響なし	影響なし	パッチ – 12.6(1)_E ReadMe
ライブデータ(LD)	CSCwa46810	パッチ：11.6.1_COP23 ReadMe	パッチ – 12.0(1)_ES18 ReadMe	パッチ – 12.5(1)_ES13 ReadMe	パッチ – 12.6(1)_E ReadMe
IDS		影響なし	影響なし	影響なし	影響なし
CUIC Co-res(CUIC-LD-IDS)	CSCwa46810	パッチ：11.6.1_COP23 ReadMe	パッチ – 12.0(1)_ES18 ReadMe	パッチ – 12.5(1)_ES13 ReadMe	パッチ – 12.6(1)_E ReadMe
CloudConnect	CSCwa51545			影響なし	パッチ – 12.6(1)_CC
ECE	CSCwa47392	影響なし	パッチ – 12.0(1)_ES6_ET2 ReadMe	パッチ – 12.5(1)_ES3_ET2 ReadMe	パッチ – 12.6(1)_E ReadMe

CCMP	CSCwa47383	影響なし	影響なし	パッチ – 12.5(1)_ES6 ReadMe	Patch-12.6(1)_ES3 ReadMe
CCDM	CSCwa47383	影響なし	影響なし	パッチ – 12.5(1)_ES6 ReadMe	パッチ – 12.6(1)_ES3 ReadMe
Google CCAI	Googleによって確認されたCCCAIフィーチャセットは影響を受けません				
Webex Experience Management(WxM)	WxMはユーザlog4jを使用しないため、ソリューションに影響はない				
カスタマーコラボレーションプラットフォーム(CCP)	CSCwa47384	影響なし	影響なし	影響なし	影響なし

**リリース日は変更される可能性があり、パッチがリリースされるまで必要に応じて更新されます*

ICMサーバでのTomcatバージョンの確認

1. ICMサーバ（ルータ、ロガー、PG、およびAWサーバ）では、「*<ICM HOME>\tomcat\bin\version.bat*」ファイルを実行して、インストールされているtomcatのバージョンを確認します。
2. tomcatバージョンが**9.0.37以降の場合**は、次の手順を実行して不具合「CSCvv73307」を修正します
3. ES_81パッチをサーバにインストールします。ICMサーバに81より大きいESがある場合は、最初にこれらのESをアンインストールしてください

- 12.5(1)_ES81パッチ – https://software.cisco.com/download/specialrelease/0aab225ecde522734cc6c6491ad1eb42

- 12.5(1)_ES81 ReadMe - https://www.cisco.com/web/software/280840583/158250/Release_Document_1.html

4. ES_81のインストールが成功したら、batファイル*"<ICM HOME>\tomcat\bin\version.bat"を実行して、tomcatのバージョンを再度確認します。*
5. tomcatバージョンはステップ1と同じままである必要があります。同じ場合は、すべての目的のESの最新の再インストールを手順どおりに進め、log4jパッチ(ES_101)を含めます

よくある質問

Q.1最新の情報を使用して文書を改訂する頻度はどのくらいですか。

解答： このドキュメントは毎日確認され、午前中（米国時間）に更新されます

Q.2 ICMバージョンは次のとおりです。（ルータ、ロガー、AW、PG）10.x、11.0(x)、11.5(x)、および11.6(1)が該当しますか。

解答：これらのバージョンは1.Xバージョンのlog4jを使用するため、影響を受けません。

> **注：**アドバイザリテーブルには、メンテナンス中のバージョンの特定のバグがリストされます。強調表示されていないバージョンはソフトウェアメンテナンスの終了であり、レビュー対象ではありません。

Q.3パッチはいつリリースされますか。

解答：アドバイザリ表は、パッチがリリースされた時点の仮日付を示しています。テーブルは、利用可能になった関連リンクで更新されます。

Q.4修正が完了するまで実装できる回避策はありますか。

解答：PSIRTのアドバイザリに従い、該当するバージョンに対してリリースされたパッチが可能な限り速やかに適用されることを推奨します。

Q.5 CUIC Standalone 11.6(1)はlog4jの影響を受けませんが、ESのreadmeには、サーバ上で必要なパッチであると記載されています。なぜですか。

正解：このESはlog4j修正のみのスタンドアロンESではありません。このES23は、VOS製品と同様の累積ESです。つまり、お客様が常に利用できる最新の累積ESは1つだけです。このシナリオでは、CuがスタンドアロンCUIC 11.6 ES 21（またはそれ以前）であり、ES22のCUIC不具合修正が必要です。この場合もES23をインストールする必要があります（ESは累積的で、最新バージョンのみ）。 さらに、このlog4j不具合はES ReadmeのLD不具合に記載されています。ESのインストール中に、必要に応じて不具合修正が導入に基づいてインストールされます(つまり、ESのインストール前にスタンドアロンCUIC/co-res CUIC/LDを確認し、それに応じて不具合修正を適用します)

Q.6組織のセキュリティスキャナの場合の対処法(例：Qualys)は、UCCE製品にパッチを適用した後にCVE-2021-45105をピックアップしますか。

解答：シスコはCVE-2021-45105を確認し、シスコ製品やクラウド製品はこの脆弱性の影響を受けないことを確認しているため、必要なアクションはありません。この情報はアドバイザリでも強調表示されています。Log4jバージョン2.16.0をDDoSに対して脆弱にするには、デフォルト以外の設定が必要です。これは、攻撃者がlog4j設定ファイルを手動で変更する必要があることを意味します。これはUCCE製品では不可能なため、CVE-2021-45105は適用されません。

Q7.システムに古いLog4j ".jar"ファイル（1.2xファイルなど）が表示された場合、どうすればよいのですか。

解答：ロールバック処理が中断されないように、古いファイルを残しておくことをお勧めします。これらのファイルの非アクティブなバージョンがシステム上にある場合、コンポーネントに脆弱性は存在しません。

ただし、ビジネスでファイルの削除が必要な場合は、実稼働環境の手順を実行して影響を最小限に抑える前に、ラボで目的のプロセスをテストすることを強く推奨します。また、バックアップとロールバックの計画は、この課題に問題が発生した場合にシステムを回復するのに役立つことを推奨します。