

CAD Java セキュリティ警告を解決して下さい

目次

[はじめに](#)

[背景説明](#)

[問題](#)

[条件](#)

[解決策](#)

[セキュリティ警告](#)

[バージョン 9.0\(2\)SU1 より前の UCCX バージョン](#)

[UCCX バージョン 9.0\(2\)SU1](#)

[UCCX バージョン 10.0\(1\)](#)

[エージェント電子メールのロギング](#)

概要

このドキュメントでは、Cisco Unified Contact Center Express (UCCX) Cisco Agent Desktop (CAD) エージェント電子メールや Cisco Agent Desktop Browser Edition (CAD-BE) で表示される Java セキュリティ警告をトラブルシューティングする方法について説明します。

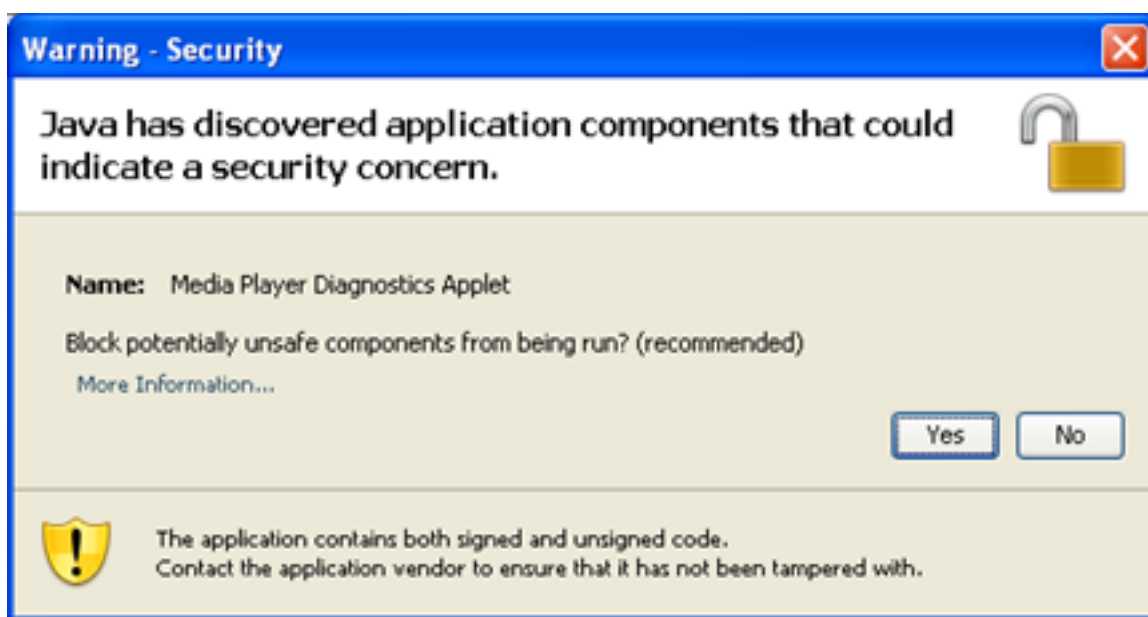
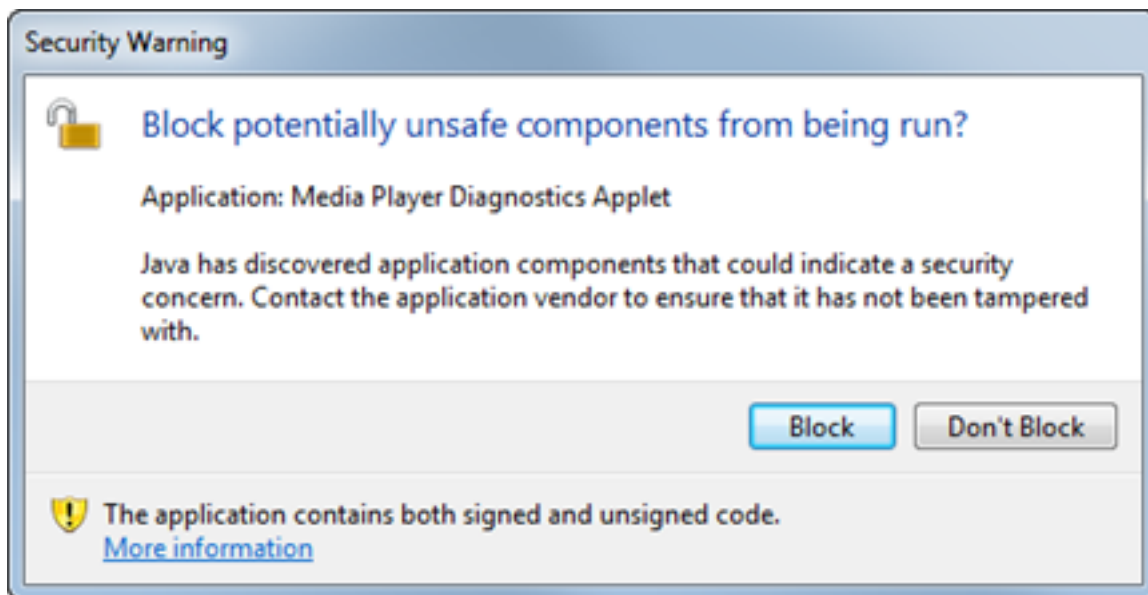
背景説明

UCCX CAD エージェント電子メールと CAD-BE は、機能するために Java (および Java アプレット) に依存しています。

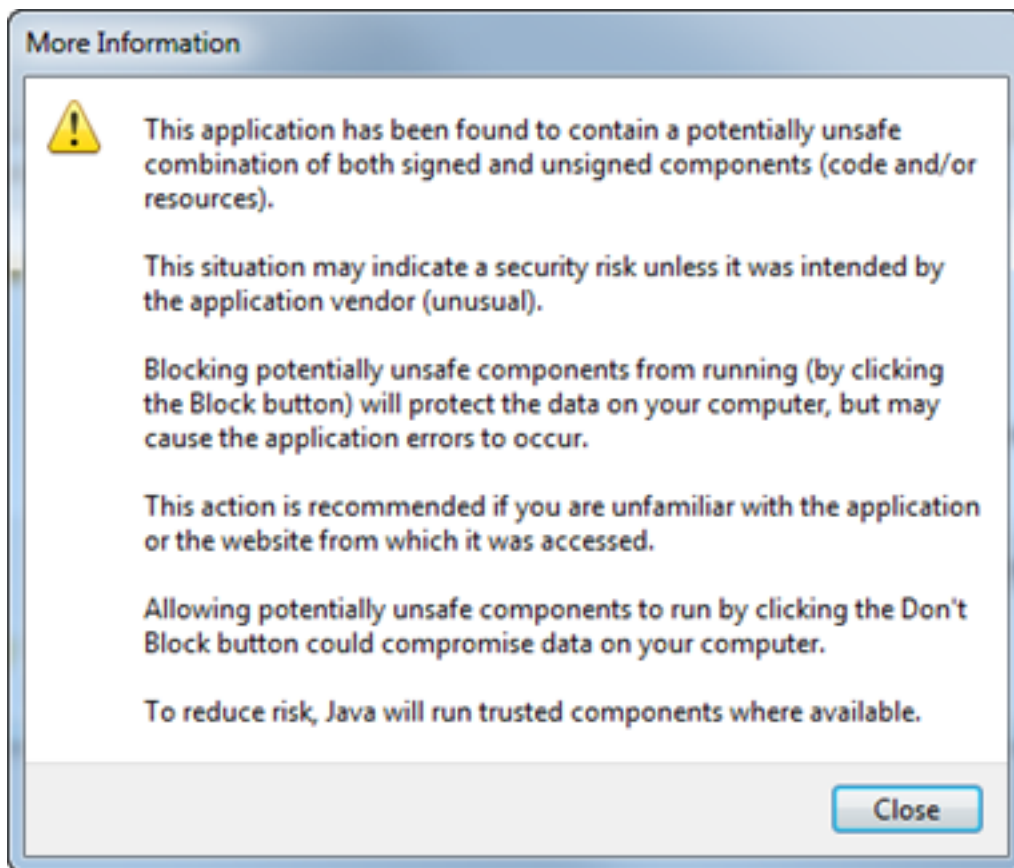
UCCX CAD エージェント電子メールと CAD-BE の一部のバージョンでサポートされる Java バージョンの Java セキュリティ ルールおよびアーキテクチャにおける変更が原因で、セキュリティ警告がユーザに表示されたり、機能が正しく機能しない、あるいはまったく機能しない事態が発生したりします。

問題

エージェント電子メールまたは CAD-BE をブラウザで実行している場合、次のような新しいセキュリティの警告が表示されます。



[More Information...] リンクをクリックすると、このメッセージが表示されます。



[Block] オプションを選択すると、アプリケーションは正常に実行されず（またはアプリケーションに完全な障害が発生します）、ブラウザ全体が動かなくなる可能性があります。[Don't block] と [No] オプションを選択したとしても、引き続き Java によって動作が制限され、ランタイムの問題を可能性があります。

条件

Java の最新リリースでは、JavaScript とアプレット間の通信を未署名コードとして処理します。これにより、CAD に署名済み/未署名の Java アプレットが混在することになり、これが原因で、ブロックするか、ブロック解除するかを選択するよう要求するセキュリティ警告が生成されます。これは、JavaScript とアプレット間の通信が存在する、すべての署名済み Java アプレットに影響します。

以下の Java リリースに、前述の変更が加えられています。

- Java リリース 1.7.0 アップデート 21 以降
- Java リリース 1.6.0 アップデート 45 以降

注: CAD では、エージェント電子メール、Cisco Supervisor Desktop、および CAD-BE で Java Runtime Environment (JRE) が使用されます。

解決策

このセクションでは、前のセクションで説明した問題の回避策について説明します。

セキュリティ警告

このセクションでは、各 UCCX バージョンでのセキュリティ ポップアップ警告をトラブルシューティングする方法について説明します。

バージョン 9.0(2)SU1 より前の UCCX バージョン

バージョン 9.0(2)SU1 より前の UCCX バージョンでは、バージョン 1.6.0 アップデート 31 までの Java しかサポートしないため、影響を受ける Java バージョンを現在実行しているインストールは、サポートされないバージョンの Java を使用していることとなります。

この問題を回避するために、マシンから Java を完全にアンインストールすることができます。CAD、CSD、および CAD-BE にログインするときに、正しい Java バージョンがインストールされます。サポートされる Java バージョンがインストールされた後、セキュリティ ポップアップ警告は表示されなくなるはずですが。

注: 最新の Java バージョンにマシンが直接更新される場合 (Java をアンインストールせずに)、ポップアップの問題が引き続き発生し、エージェント電子メールが意図したように動作しない可能性があります。

UCCX バージョン 9.0(2)SU1

UCCX バージョン 9.0(2)SU1 では、Java バージョン 1.6.0 アップデート 45 をサポートし、Cisco Bug ID [CSCug80029](#) の修正が含まれています。

PC で Java バージョン 1.6.0 アップデート 45 が実行されている場合、セキュリティ ポップアップ警告は表示されず、エージェント電子メールは正常に機能するはずですが。

UCCX バージョン 10.0(1)

UCCX バージョン 10.0(1) は Java バージョン 1.7.0 アップデート 45 をサポートします。最近、Java バージョン 1.7.0 アップデート 51 がリリースされました。その時点で、Oracle はセキュリティ ベースラインをアップデート 51 に引き上げました。これによりアップデート 45 は「安全でない」に分類されます。UCCX バージョン 10.0(1) と Java バージョン 1.7.0 アップデート 45 を実行する場合、エージェント電子メールにログインすると、セキュリティ ポップアップ警告が表示されます。

この問題を回避するには、ブラウザのセキュリティ スライドを [Medium] まで下げ、エージェント電子メールが正常に機能するように、メッセージを受け取るたびに [Don't Block] をクリックする必要があります。また、この問題を解決するために、Java バージョン 1.7.0 アップデート 51 にアップグレードすることもできます。Oracle BugID [JDK-8027405](#) で説明されている修正 (アップデート 51 に含まれています) によって、今後この問題は防止されるはずですが。

ヒント : 詳細については、Cisco Bug ID [CSCum69044](#) を参照してください。

エージェント電子メールのロギング

Java バージョン 1.7.0 アップデート 45 が UCCX バージョン 10.0 の CAD に統合されると、Oracle による JRE での変更が原因で、Cisco Bug ID [CSCum00334](#) で説明されている問題が検出されました。この問題により、エージェント電子メールのクライアント側のログ (`EEMUI*.log`) がデフォルトで無効にされる問題が発生しました。

問題の概要を次に示します。

- リリース 7u21 では、セキュリティ ポップアップ警告の発生を防ぐために、JRE で *Trusted-Library* マニフェスト属性を使用する必要がありました。CAD の内部開発では、問題を軽減するためにこの属性が使用され、問題は生じませんでした。
- リリース 7u45 では、新しいセキュリティ ポップアップ警告の発生を防ぐために、JRE で *Caller-Allowable-Codebase* マニフェスト属性も使用する必要が生じました。
- JRE リリース 7u45 では *Trusted-Library* と *Caller-Allowable-Codebase* マニフェスト属性が共存できないという問題が、Oracle JDK のバグで説明されています。共存した場合、後者の属性は無視されます。
- Oracle の回避策は、*Caller-Allowable-Codebase* マニフェスト属性のみを使用するというもので、これにより、両方のセキュリティ ポップアップ警告の発生を防ぐことができるはずでした。しかし、この回避策を実装した場合、ロギング サブシステムを初期化するために必要な `.jar` マニフェスト ファイルにアクセスしようとする、`EemUi` に対して最初のセキュリティ ポップアップ警告がトリガーされます。

ヒント：この問題の詳細については、「[Java プラットフォーム グループ、製品管理ブログ](#)」を参照してください。

Oracle では、バグ ID [JDK-8026347](#) でこの問題を追跡し、解決する予定です。

注: このバグは、バグ ID [JDK-8026228](#) と重複しています。ただし、このバグは正式に登録しないと表示できません。

バグ ID [JDK-8026228](#) が修正されると、CAD で *Trusted-Library* と *Caller-Allowable-Codebase* の両方のマニフェスト属性を同時に使用できるようになる予定です。これにより、ロギング サブシステムが使用されても、最初のセキュリティ ポップアップ警告が表示されなくなります (JRE バージョン 7u21 での *Trusted-Library* マニフェスト属性の追加により、このセキュリティ ポップアップ警告の軽減に成功しているため)。

ヒント：CAD エージェント電子メールで UCCX バージョン 10.0 が使用され、クライアント側のデバッグが必要になる場合、Cisco Bug ID [CSCum00334](#) を参照してください。