Microsoft KB3161608/KB3161639 のインストール後に CUIC の Web ページが IE 11 にロードされない

目次

概要

このドキュメントでは、Microsoft サポート技術情報（KB）更新をインストールした後、Cisco Unified Intelligence Center（CUIC）Web ページが Internet Explorer（IE）をロードしなくなるというシナリオについて説明します。

また、CUIC の観点から、考えられえる回避策/解決策も説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- Windows の管理
- CUIC の管理および設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

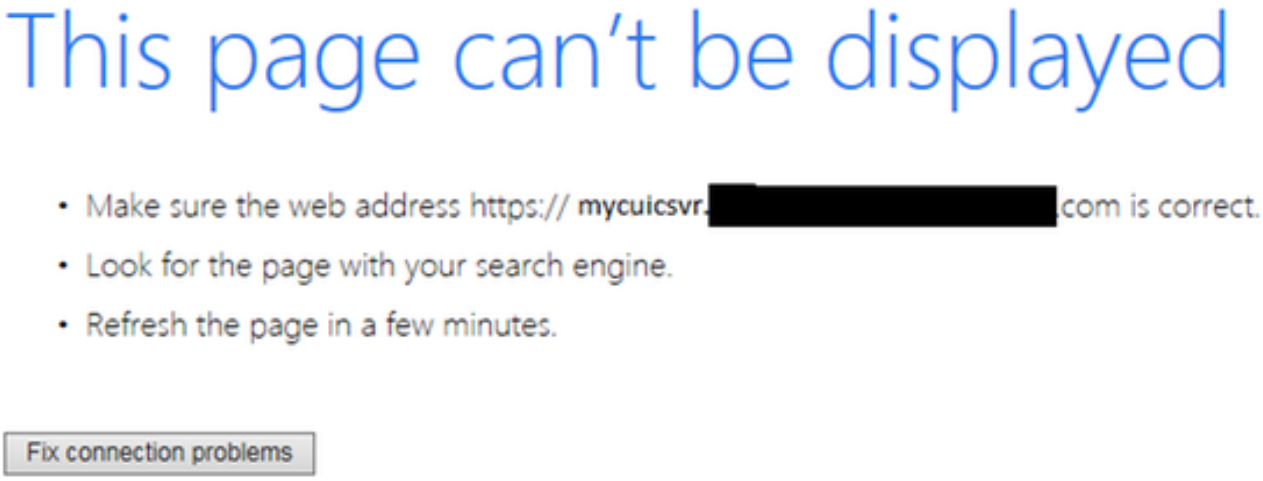
- Cisco Unified Intelligence Center 10.5(1)
- Cisco Unified Intelligence Center 10.x
- Cisco Unified Intelligence Center 9.1(x)
- Windows 7、Windows 8
- Internet Explorer 11

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

シナリオ

- CUIC バージョン 9.1(1) または CUIC バージョン 10.5(1)
- Windows 7 または Windows 8 上の Internet Explorer（IE）バージョン 11
- Windows 7/8 に KB3161639 をインストール
- Internet Explorer で CUIC のリンク（http://<CUIC HOST ADDRESS>/*cuic*）を起動

以下の図に示すエラー メッセージとプロンプトが表示されます。



分析

Microsoft では 2016 年 6 月の更新ロールアップ KB3161608 の一部として新しい暗号スイートを追加しました。

Cipher suite	FIPS mode enabled	Protocols	Exchange	Encryption	Hash
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Yes	TLS 1.2, TLS 1.1, TLS 1.0	DHE	AES	SHA1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Yes	TLS 1.2, TLS 1.1, TLS 1.0	DHE	AES	SHA1

KB3161639 に含まれる **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** および **TLS_DHE_RSA_WITH_AES_256_CBC_SHA** が暗号スイートに追加され、Windows OS での暗号スイートのデフォルト優先順位が変更されています。

このことから、クライアント マシンが上記の更新を適用すると、クライアントは CUIC Tomcat サーバと **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** を使用して通信するようになります（CUIC Tomcat コネクタ設定で **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** が定義されているため）。

ただし、**TLS_DHE_RSA_WITH_AES_128_CBC_SHA** 暗号を使用した通信は機能しません。 その理由は、Microsoft が口グイン攻撃を回避するために適用する Diffie Hellman Exchange（DHE）キー長の最小要件は 1024 ビットであるためです。

バージョン 11.x までの CUIC で使用している Java 6 バージョンでは 768 ビットのキーのみがサポートされます。 そのため、これが原因でハンドシェイクが失敗します。

解決策

この解決策は、問題が解決されている CUIC 11.0(1) には適用されません。 CUIC バージョン 9.1(1) および 10.x バージョンでは、ここから入手できる OpenSSL COP ファイルによって問題を解決できます。

OpenSSL COP ファイルではログイン攻撃を回避するための **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** が削除されるため、CUIC Tomcat コネクタから Diffie-Hellman（DHE）暗号サポートが削除されます。