CUIC Web ページは Microsoft KB3161608/KB3161639 のインストールの後で IE 11 でロードしません

目次

概要

この資料は Cisco Unified Intelligence Center（CUIC）Web ページが Microsoft Knowledge Base（KB）更新のインストールの後で Internet Explorer（IE）でロードすることを止めるシナリオを解説していたものです。

技術情報はまた CUIC の観点からの可能性のある回避策/ソリューションを提供します。

前提条件

要件

Cisco はこれらのトピックのナレッジがあることを推奨します:

- Windows 管理
- CUIC 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。

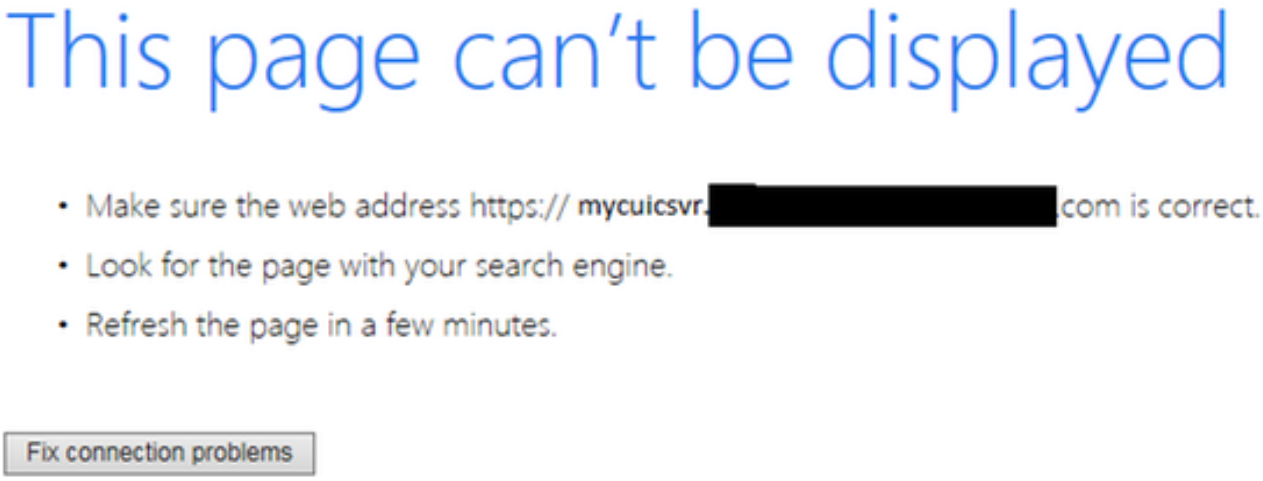
- Cisco Unified Intelligence Center 10.5(1)
- Cisco Unified Intelligence Center 10.x
- Cisco Unified Intelligence Center 9.1(x)
- Windows 7 か 8
- Internet Explorer 11

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)か CUIC バージョン 10.5(1)
- Windows 7 または Windows 8 の Internet Explorer （ IE ） 11
- Windows 7 /8 で KB3161639 をインストールして下さい
- Internet Explorer の CUIC リンクを- http:// <CUIC ホスト・ アドレス *>/cuic* 起動させて下さい

これはイメージに示すようにエラーメッセージとプロンプト表示します:



分析

Microsoft は 2016 年 6 月アップデート巻き上げ KB3161608 の一部として、イメージに示すように、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 の一部として、**TLS_DHE_RSA_WITH_AES_128_CBC_SHA** および **TLS_DHE_RSA_WITH_AES_256_CBC_SHA は**暗号スイートに追加され、暗号スイートのデフォルトプライオリティ発注は Windows OS で変更されます。

このような理由で（ **TLS_DHE_RSA_WITH_AES_128_CBC_SHA が** CUIC Tomcat コネクタ構成で定義されると同時に）クライアントマシンが上記の更新を備えていれば、CUIC Tomcat サーバと **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** を使用して通信しがちです。

ただし、**TLS_DHE_RSA_WITH_AES_128_CBC_SHA** 暗号を使用して通信ははたらきません。 これは停滞不正侵入を固定するために Microsoft によって実施される Diffie Hellman Exchange （ DHE ）キーのための 1024 ビット最小限の要件が理由でそうなったものです。

バージョン 11.x に 768 のビット キーだけをサポートする Java が 6 つのバージョンあるまで

CUIC。 従って、それによりハンドシェイク失敗を引き起こす場合があります。

解決策

これは CUIC 11.0(1) へこの問題が解決されるところに適用されないです。 CUIC バージョン 9.1(1) および 10.x バージョンに関しては、これは利用可能な開いた SSL COPS ファイルによってここに解決されます

openssl 警察官の一部として、Diffie Hellman （DHE）暗号サポートは CUIC Tomcat コネクタから停滞不正侵入を防ぐために TLS_DHE_RSA_WITH_AES_128_CBC_SHA を取除くことによって取除かれます。