

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[シナリオ](#)

[分析](#)

[解決策](#)

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

このドキュメントの情報は、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、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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 の起動 CUIC リンク- [http:// <CUICホストアドレス>/cuic](http://<CUICホストアドレス>/cuic)
- 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:

This page can't be displayed

- Make sure the web address `https:// mycuicsvr. [REDACTED] com` is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Fix connection problems

?

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きません。これは [停滯攻撃を固定するために 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。

[768 のビット キーだけを](#) サポートするバージョン 11.x に Java 6 バージョンがあるまで 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 CUIIC 11.0(1) へこの問題が解決される場所に適用されません。CUIIC 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、デフィーヘルマン (DHE) 暗号サポートは CUIIC Tomcat コネクタから停滞攻撃を防ぐために TLS_DHE_RSA_WITH_AES_128_CBC_SHA を取除くことによって取除かれます。