安裝Microsoft KB3161608/KB3161639後，CUIC網頁未載入到IE 11

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[案例](#)
[分析](#)
[解決方案](#)

簡介

本文檔介紹在安裝Microsoft知識庫(KB)更新後，Cisco Unified Intelligence Center(CUIC)網頁停止載入到Internet Explorer(IE)中的情況。

文章還從CUIC的角度提供了可能的變通辦法/解決方案。

必要條件

需求

思科建議您瞭解以下主題：

- Windows管理
- CUIC管理和配置

採用元件

本檔案中的資訊是根據以下軟體版本：

- 思科整合情報中心10.5(1)
- 思科整合情報中心10.x
- 思科整合情報中心9.1(x)
- Windows 7或8
- Internet Explorer 11

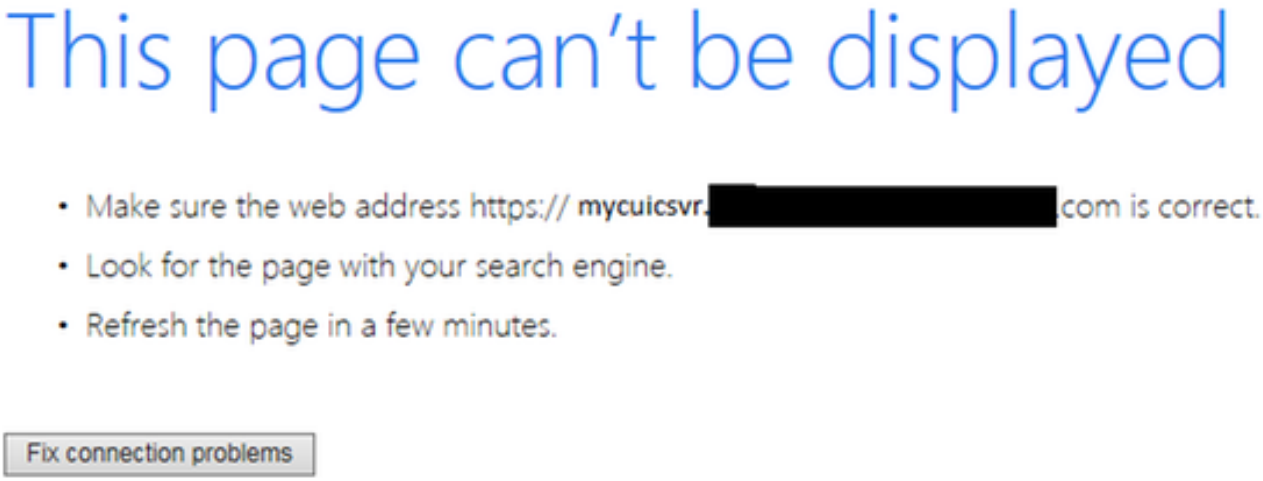
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

案例

- CUIC版本9.1(1)或CUIC版本10.5(1)

- Windows 7或Windows 8上的Internet Explorer(IE)11
- 在Windows 7/8上安裝KB3161639
- 在Internet Explorer上啟動CUIC連結- http://<CUIC主機地址>/*cuic*

如下圖所示的錯誤消息提示：



分析

Microsoft在2016年6月更新彙總KB3161608中增加了新的密碼套件，如圖所示。

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

作為KB3161639的一部分，將**TLS_DHE_RSA_WITH_AES_128_CBC_SHA**和**TLS_DHE_RSA_WITH_AES_256_CBC_SHA**新增到密碼套件中，並在Windows作業系統中更改密碼套件的預設優先順序順序。

因此，如果客戶端電腦具有上述更新，則它們傾向於使用**TLS_DHE_RSA_WITH_AES_128_CBC_SHA**與CUIC tomcat伺服器進行通訊(因為**TLS_DHE_RSA_WITH_AES_128_CBC_SHA**在其CUIC tomcat聯結器配置中定義)。

但是，使用**TLS_DHE_RSA_WITH_AES_128_CBC_SHA密碼的通訊**不起作用。這是因為Microsoft強制實施針對Diffie Hellman Exchange(DHE)金鑰的1024位最低要求來修復登入攻擊。

CUIC直到版本11.x都具有Java 6版本，該版本僅支援768位金鑰。因此，它可以導致握手失敗。

解決方案

這不適用於解決此問題的CUIC 11.0(1)。對於CUIC版本9.1(1)和10.x版本，可通過此處提供的開啟SSL COP檔案解決此問題

作為openssl cop的一部分，通過刪除TLS_DHE_RSA_WITH_AES_128_CBC_SHA來防止Diffie-Hellman(DHE)密碼支援從CUIC tomcat聯結器刪除，以防止日誌堵塞攻擊。