La pagina Web CUIC non viene caricata su IE 11 dopo l'installazione di Microsoft KB3161608/KB3161639

Sommario

Introduzione

In questo documento vengono descritti gli scenari in cui le pagine Web di Cisco Unified Intelligence Center (CUIC) non vengono più caricate in Internet Explorer dopo l'installazione degli aggiornamenti della Microsoft Knowledge Base (KB).

L'articolo offre anche soluzioni alternative dal punto di vista di CUIC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione di Windows
- Amministrazione e configurazione CUIC

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

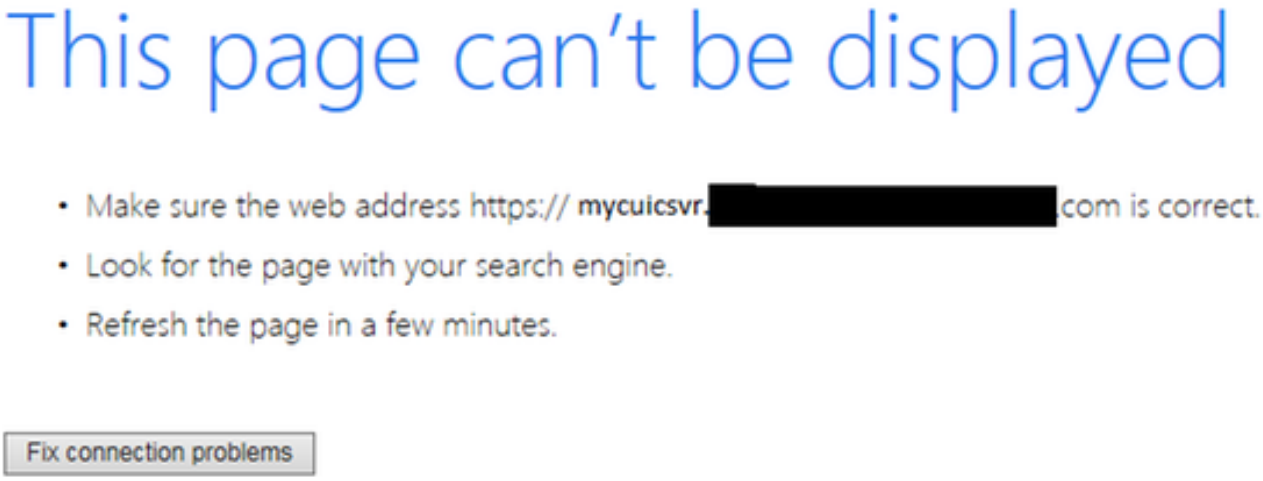
- Cisco Unified Intelligence Center 10.5(1)
- Cisco Unified Intelligence Center 10.x
- Cisco Unified Intelligence Center 9.1(x)
- Windows 7 o 8
- Internet Explorer 11

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Scenario

- CUIC versione 9.1(1) o CUIC versione 10.5(1)
- Internet Explorer (IE) 11 su Windows 7 o Windows 8
- Installa KB3161639 in Windows 7/8
- Avvia collegamento CUIC su Internet Explorer - http://<CUIC HOST ADDRESS>/*cuic*

Viene visualizzato il messaggio di errore mostrato nell'immagine:



Analisi

Microsoft ha aggiunto le nuove suite di cifratura, come mostrato nell'immagine, come parte dell'aggiornamento cumulativo di giugno 2016 KB3161608.

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

Come parte di KB3161639, **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** e **TLS_DHE_RSA_WITH_AES_256_CBC_SHA** vengono aggiunti alle suite di cifratura e l'ordine di priorità predefinito delle suite di cifratura viene modificato nel sistema operativo Windows.

Per questo motivo, se i computer client dispongono degli aggiornamenti di cui sopra, tendono a comunicare utilizzando **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** con CUIC tomcat server (in quanto **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** è definito nella relativa configurazione CUIC tomcat connector).

Tuttavia, la comunicazione che utilizza la cifratura **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** non funziona. Ciò è dovuto al requisito minimo di 1024 bit per le chiavi Diffie Hellman Exchange (DHE) imposto da Microsoft per correggere l'attacco logjam.

CUIC fino alla versione 11.x dispone delle versioni Java 6 che supportano solo chiavi a 768 bit. Pertanto, può causare un errore di handshake.

Soluzione

Questo non è applicabile a CUIC 11.0(1) dove il problema è risolto. Per le versioni CUIC 9.1(1) e 10.x, questa condizione viene risolta dal file COP SSL aperto disponibile qui

Come parte della copia openssl, il supporto della cifratura Diffie-Hellman (DHE) viene rimosso dal connettore CUIC tomcat rimuovendo **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** per prevenire attacchi logjam.