CUIC-webpagina wordt niet geladen op IE 11 na de installatie van Microsoft KB3161608/KB3161639

Inhoud

Inleiding

In dit document worden de scenario's beschreven waarin Cisco Unified Intelligence Center (CUIC) webpagina's stoppen met laden op Internet Explorer (IE) na de installatie van Microsoft KennBase (KB)-updates.

Het artikel biedt ook mogelijke oplossingen/oplossingen vanuit het gezichtspunt van de CUIC.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis over deze onderwerpen te hebben:

- Windows-beheer
- CUIC-beheer en -configuratie

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

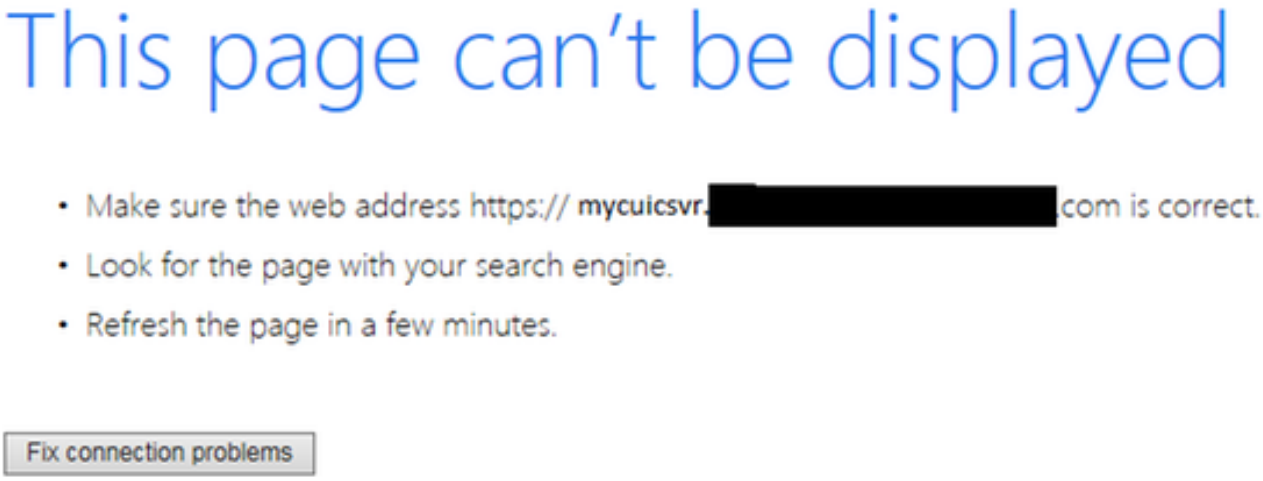
- Cisco Unified Intelligence Center versie 10.5(1)
- Cisco Unified Intelligence Center versie 10.x
- Cisco Unified Intelligence Center 9.1(x)
- Windows 7 of 8
- Internet Explorer 11

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Scenario

- CUIC versie 9.1(1) of CUIC versie 10.5(1)
- Internet Explorer (IE) 11 op Windows 7 of Windows 8
- Installeer KB3161639 op Windows 7/8
- CUIC-link starten op Internet Explorer - http://<CUIC HOST ADRES>/*cuic*

Dit leidt tot een foutmelding zoals in de afbeelding:



Analyse

Microsoft voegde de nieuwe conceptversies, zoals in de afbeelding, toe als onderdeel van de in juni 2016 gepubliceerde update rollup 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

Als onderdeel van KB3161639 worden **TLS_DHE_RSA_MET_AES_128_CBC_SHA** en **TLS_DHE_RSA_MET_AES_256_CBC_SHA** toegevoegd aan de reeks-formaten en de standaard prioriteitsvolgorde van Cipher worden gewijzigd in Windows OS.

Vanwege dit feit als clientmachines de bovenstaande updates hebben, hebben ze de neiging te communiceren met **TLS_DHE_RSA_MET_AES_128_CBC_SHA** met CUIC-server (zoals **TLS_DHE_RSA_MET_AES_128_CBC_SHA** is gedefinieerd in de CUICcat-connector).

De communicatie met **het** algoritme TLS_DHE_RSA_MET_AES_128_CBC_SHA werkt niet. Dit komt door de minimaal vereiste van 1024 bit voor de Diffie Hellman Exchange (DHE) toetsen die door Microsoft worden afgedwongen om de logjam-aanval te repareren.

CUIC tot versie 11.x heeft Java 6 versies die alleen 768 bit-toetsen ondersteunen. Hierdoor kan

een handdruk falen.

Oplossing

Dit is niet van toepassing op CUIC 11.0(1) waar dit probleem is opgelost. Voor CUIC-versies 9.1(1) en 10.x-versies wordt dit opgelost door het open SSL COP-bestand dat hier beschikbaar is

Als onderdeel van openssl cop wordt de ondersteuning van het DIffie-Hellman (DHE) algoritme verwijderd van de CUIC naar de connector door TLS_DHE_RSA_MET_AES_128_CBC_SHA te verwijderen om een logjam-aanval te voorkomen.