O Web page CUIC não carrega em IE 11 após a instalação do Microsoft KB3161608/KB3161639

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Cenário](#)
[Análise](#)
[Solução](#)

Introdução

Este original descreve as encenações em que Cisco unificou a carga Center da parada dos Web pages da inteligência (CUIC) no internet explorer (IE) após as atualizações da base de conhecimento da instalação do Microsoft (KB).

O artigo igualmente oferece ações alternativas/soluções potenciais da perspectiva do CUIC.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento nestes assuntos:

- A administração de Windows
- A administração e configuração CUIC

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

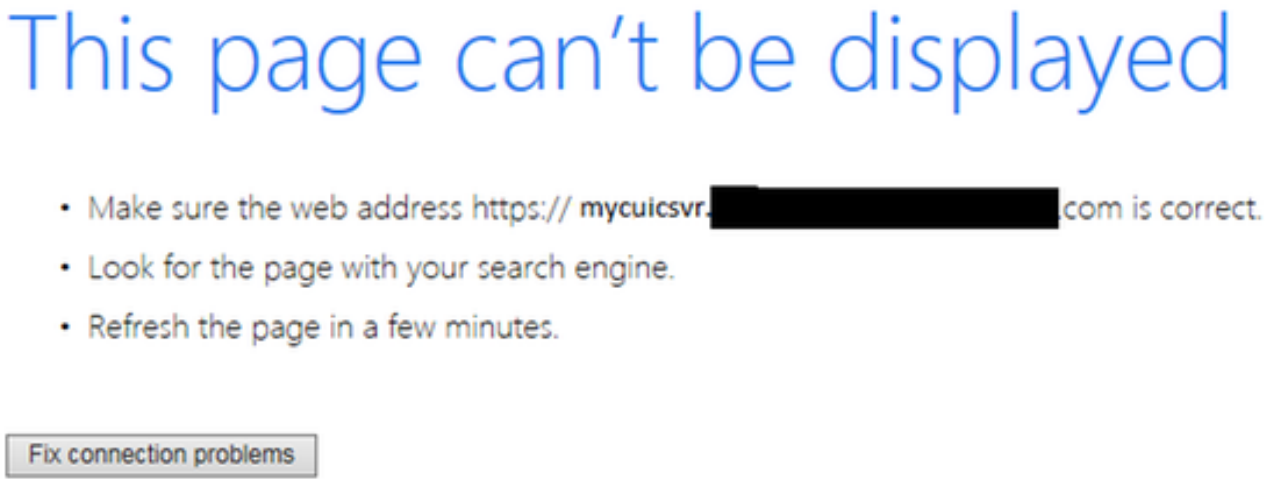
- Cisco unificou o centro da inteligência 10.5(1)
- Cisco unificou a inteligência 10.x Center
- Cisco unificou o centro da inteligência 9.1(x)
- Windows 7 ou 8
- Internet explorer 11

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Cenário

- Versão 9.1(1) CUIC ou versão 10.5(1) CUIC
- Internet explorer (IE) 11 em Windows 7 ou em Windows 8
- Instale KB3161639 em Windows 7/8
- Link do lançamento CUIC no internet explorer - ENDEREÇO DE HOST *>/cuic de* http://<CUIC

Isto alerta com o Mensagem de Erro segundo as indicações da imagem:



Análise

Microsoft adicionou as séries novas da cifra, segundo as indicações da imagem, como parte de um rollup KB3161608 da atualização do de junho de 2016.

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

Como parte de KB3161639, **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** e **TLS_DHE_RSA_WITH_AES_256_CBC_SHA** são adicionados às séries da cifra e a ordem da prioridade padrão de séries da cifra é mudada no SO Windows.

Devido a isto se as máquinas cliente têm as atualizações acima, tendem a comunicar-se usando **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** com o server CUIC TomCat (enquanto **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** é definido em sua configuração do conector CUIC TomCat).

Contudo, a comunicação que usa a cifra **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** não trabalha. Isto é devido ao requisito mínimo de 1024 bit para as chaves da troca do Diffie Hellman (DHE) reforçadas por Microsoft para fixar o ataque do atasco.

CUIC até que a versão 11.x tiver as versões das Javas 6 que apoia somente 768 chaves do bit. Assim, pode causar uma falha do aperto de mão.

Solução

Isto não é aplicável a CUIC 11.0(1) onde esta edição é resolved. Para versões das versões 9.1(1) e 10.x CUIC, isto é resolvido pelo arquivo aberto da BOBINA SSL disponível aqui

Como parte da bobina do OpenSSL, o apoio da cifra de Diffie-Hellman (DHE) é removido do conector CUIC TomCat removendo **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** para impedir o ataque do atasco.