Contents

Introduction

This document describes the scenarios in which Cisco Unified Intelligence Center (CUIC) webpages stop loading on Internet Explorer (IE) after the installation of Microsoft Knowledge Base (KB) updates.

The article also offers potential workarounds/solutions from the CUIC's perspective.

Prerequisites

Requirements

Cisco recommends that you have knowledge on these topics:

- Windows Administration
- CUIC Administration and Configuration

Components Used

The information in this document is based on these software versions:

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

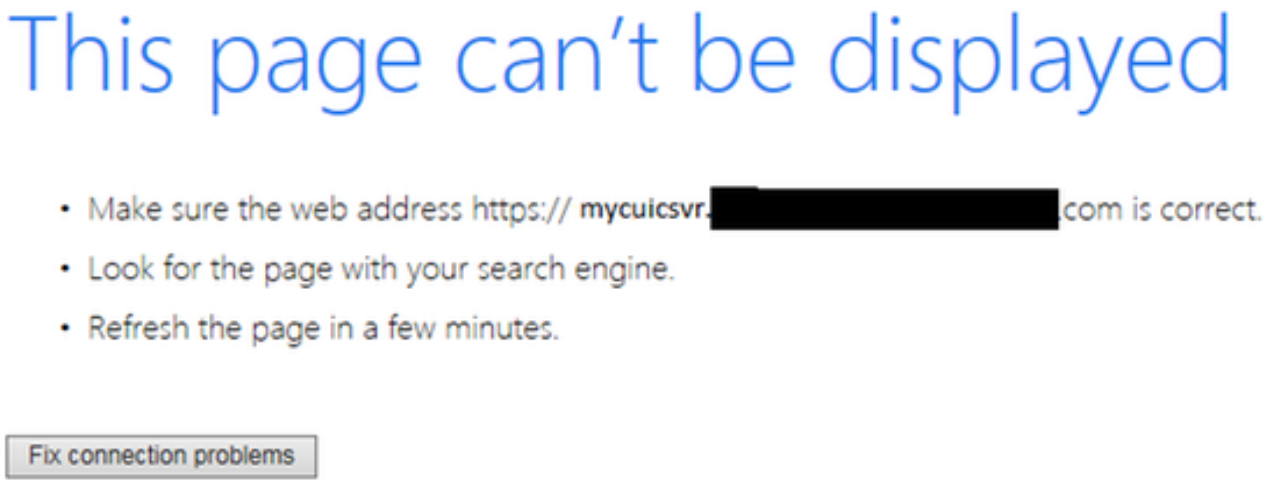
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Scenario

- CUIC version 9.1(1) or CUIC version 10.5(1)
- Internet Explorer (IE) 11 on Windows 7 or Windows 8
- Install KB3161639 on Windows 7/8

- Launch CUIC link on Internet Explorer - http://<CUIC HOST ADDRESS>/*cuic*

This prompts with the error message as shown in the image:



Analysis

Microsoft added the new Cipher suites, as shown in the image, as a part of June 2016 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

As part of KB3161639, **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** and **TLS_DHE_RSA_WITH_AES_256_CBC_SHA** are added to the cipher suites and the default priority order of Cipher suites are changed in the Windows OS.

Because of this if client machines have the above updates, they tend to communicate using **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** with CUIC tomcat server (as **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** is defined in its CUIC tomcat connector config).

However, the communication using **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** cipher does not work. This is because of the 1024 bit minimum requirement for the Diffie Hellman Exchange (DHE) keys enforced by Microsoft to fix the logjam attack.

CUIC until version 11.x has the Java 6 versions which only supports 768 bit keys. Thus, it can cause a handshake failure.

Solution

This is not applicable to CUIC 11.0(1) where this issue is resolved. For CUIC versions 9.1(1) and

10.x versions, this is resolved by the open SSL COP file available here

As part of openssl cop, the Diffie-Hellman (DHE) cipher support is removed from CUIC tomcat connector by removing **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** to prevent logjam attack.