CUIC网页在IE 11不装载在Microsoft以后KB3161608/KB3161639的安装

Contents

Introduction

本文描述Cisco Unified智力中心的方案(CUIC)网页停止装载在Internet Explorer (IE)在Microsoft知识库(KB)更新的安装以后。

条款也提供潜在解决方法/解决方案从CUIC的方面。

Prerequisites

Requirements

Cisco建议您有在这些题目的知识：

- Windows管理
- CUIC管理和配置

Components Used

本文档中的信息基于以下软件版本：

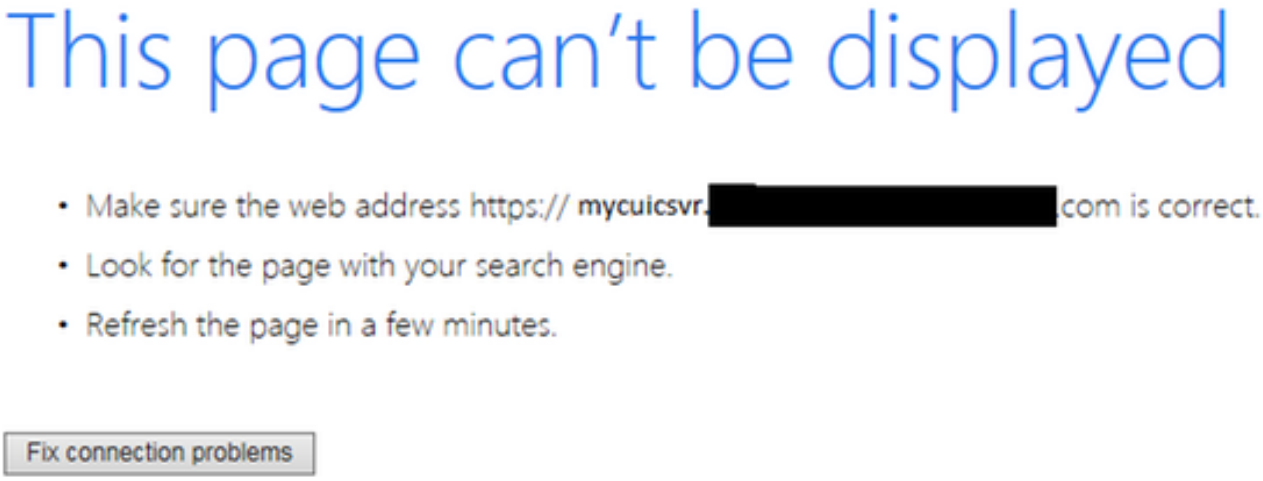
- Cisco Unified智力中心10.5(1)
- Cisco Unified智力中心10.x
- Cisco Unified智力中心9.1(x)
- Windows 7或8
- Internet Explorer 11

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.

场景

- CUIC版本9.1(1)或CUIC版本10.5(1)
- 在Windows 7或Windows 8的Internet Explorer (IE) 11
- 在Windows 7/8上安装KB3161639
- 启动在Internet Explorer的CUIC链路- http:// <CUIC主机地址>/*cuic*

如镜像所显示，这提示与错误信息：



分析

如镜像所显示， Microsoft添加了新的密码套件，作为2016年6月更新纵向分配KB3161608的部分。

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

作为KB3161639一部分， **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**和 **TLS_DHE_RSA_WITH_AES_256_CBC_SHA**被添加到密码套件，并且密码套件默认优先级定货在Windows OS更改。

因此，如果客户端机器有上述更新，他们倾向于联络使用 **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**与CUIC Tomcat服务器(当 **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**在其CUIC Tomcat连接器设置被定义)。

然而，通信使用**TLS_DHE_RSA_WITH_AES_128_CBC_SHA**密码不工作。这是由于Microsoft强制执行的Dffie Hellman Exchange (DHE)键的1024位最低要求修正木材堵塞攻击。

CUIC，直到版本11.x有只支持768个位键的Java 6个版本。因此，它能导致握手故障。

解决方案

这不是可适用的对CUIC 11.0(1)此问题是解决的地方。对于CUIC版本9.1(1)和10.x版本，开放SSL

COPS可用文件解决这这里

作为openssl策略一部分， Diffie-Hellman (DHE)密码技术支持从CUIC Tomcat连接器被取消被去除 TLS_DHE_RSA_WITH_AES_128_CBC_SHA防止木材堵塞攻击。