目录

简介

本文描述Cisco Unified智能中心的方案(CUIC)网页在Internet Explorer (IE)的终止加载在Microsoft知识库以后(KB)安装更新。

条款也提供潜在应急方案/解决方案从CUIC的方面。

先决条件

要求

思科建议您有在这些主题的知识：

- Windows管理
- CUIC管理和配置

使用的组件

本文档中的信息基于以下软件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

方案

- 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的安装KB3161639
- 在Internet Explorer的启动CUIC链路- http:// <CUIC主机地址>/*cuic*

如镜像所显示，这提示与错误消息：

This page can't be displayed

??

分析

如镜像所显示， Microsoft添加了新的密码器套件，六月2016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**被添加到密码器套件，并且密码器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，他们倾向于通信使用 **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**用CUIC Tomcat服务器(当 **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**在其CUIC Tomcat连接器设置定义)。

然而，通信使用**TLS_DHE_RSA_WITH_AES_128_CBC_SHA**密码器不工作。这是由于Microsoft强制执行的Dffie Hellman Exchange (DHE)密钥的1024个位最低要求修复木材堵塞攻击。

CUIC，直到版本11.x有只支持768位密钥的Java 6个版本。因此，它能导致握手失败。

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可用文件解决这此处

作为openssl策略一部分， Diffie-Hellman (DHE)密码器支持从CUIC Tomcat连接器删除通过删除 **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**防止木材堵塞攻击。