

UCCX 10.6页在IE11不加载在Microsoft以后 KB3161608/KB3161606的安装

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[场景 1](#)

[结果](#)

[场景 2](#)

[结果](#)

[分析](#)

Introduction

本文描述能导致不装载Cisco Unified Contact Center Express的方案(UCCX)并且/或者精良的网页，UCCX 10.6的版本安装。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Windows管理
- UCCX管理和配置

Components Used

本文档中的信息基于以下软件版本：

- Cisco Unified Contact Center Express 10.6(1)
- Cisco Unified Contact Center Express 10.6(1) SU1
- 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 1

- 与安全散列算法的UCCX 10.6(1)基本版本(SHA)1或SHA256认证

- Windows的7或8 Internet Explorer (IE) 11
- 在Windows 8的Windows 7或KB3161606上安装KB3161608

结果

当您连接时在IE11的UCCX Web Admin或精良登录页导致显示“此页的此消息不可能显示”。

This page can't be displayed

- Make sure the web address `https://uccx106base [REDACTED].com` is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Fix connection problems

场景 2

- UCCX 10.6(1) SU1与SHA1或SHA256认证
- Windows的7或8 IE11
- 在Windows 8的Windows 7或KB3161606上安装KB3161608

结果

此方案结果到此：

- UCCX Web管理员页面被载入并且允许您顺利地登陆。
- 精良登录页被载入并且允许用户输入证件。然而，精良提示用户接受7443证书，但是页用同一个消息不加载-“此页不可能显示”。

This page can't be displayed

- Make sure the web address `https://uccx106[REDACTED]:7443` is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Fix connection problems

分析

KB实际上是一特别是安装此KB3161639更新添加新的密码套件到Internet Explorer和Microsoft边缘在Windows的一盒更新。当您仔细地看此KB，这两个传输层安全(TLS)密码套件被添加到IE使用的一个列表：TLS_DHE_RSA_WITH_AES_128_CBC_SHA和TLS_DHE_RSA_WITH_AES_256_CBC_SHA。

在Firefox这些可以是失效的通过此程序：

1. 连接对大约：设置。
2. 搜索security.ssl3.dhe由于。
3. 在设置他们的security.ssl3.dhe_rsa_aes_256_sha和security.ssl3.dhe_rsa_aes_128_sha的双击对错误。

然而与IE11没有可以通过浏览器完成的解决方法。反而，管理员修改本地或域组策略排除在SSL配置的密码。

为了通过gpedit.msc Windows模块修改本地策略，请连接对Computer Configuration >Administrative工具>Network >SSL配置设置>SSL密码套件命令。

如果设置套件命令失效或那么没有被配置得默认顺序使用和对UCCX/Finesse的块访问。反而，应该设置这到启用，并且应该修改密码套件命令排除以上提到的两个密码。注释限制将使用密码列表，因为他们不可以超出长度1023个字符。已知的密码列表与UCCX/Finesse 10.6一起使用是作为这些：

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,  
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,  
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,  
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,  
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,  
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384,  
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384,  
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,  
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,  
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,  
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,
```

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_CK_DES_192_EDE3_CBC_WITH_MD5

其它选项是从需要访问精良或UCCX Web Admin的所有机器去除KB3161608或KB3161606。

此问题在UCCX 10.6(1) SU2或11.0不提交，木材堵塞弱点在这些版本被修正了。有与此问题产生关联的缺陷， [CSCuv89545](#)，在UCCX 10.6 SU1 ES02和SU2被解决。一个相关缺陷， [CSCuu82538](#)，在管理红帽子企业6的虚拟机被解决作为客户OS。

Note:为Windows 10 (KB3163018)的一次相似的更新在UCCX版本10.6和10.6 SU1也导致此问题出现，当曾经IE11时。然而， Windows 10不是UCCX的这些版本的一个支持的操作系统，并且不应该使用。当使用时Windows 10，问题可以是解决的，如果使用Firefox，升级UCCX到版本10.6 SU2或去除KB更新