

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

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[场景 1](#)

[结果](#)

[场景 2](#)

[结果](#)

[分析](#)

简介

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，版本UCCX 10.6安装。

先决条件

要求

Cisco 建议您了解以下主题：

- Windows管理
- UCCX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 Contact Center Express 10.6(1)
- Cisco Unified Contact Center Express 10.6(1) SU1
- 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。

场景 1

- 与安全散列算法的UCCX 10.6(1)基本版本(SHA)1或SHA256证书
- Windows的7或8 Internet Explorer (IE) 11

- 在Windows 7或KB3161606的安装KB3161608在Windows 8

结果

当您导航时在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证书
- Windows的7或8 IE11
- 在Windows 7或KB3161606的安装KB3161608在Windows 8

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凭证。然而，精良提示用户接受7443证书，但是页不加载与同一个消息-“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实际上是特别是安装此一KB3161639更新添加新建的密码器套件到Internet Explorer和Microsoft边缘Windows的一盒更新。当您仔细地看此KB，这两个传输层安全(TLS)密码器套件被添加到IE:使用的的一个的列表TLS_DHE_RSA_WITH_AES_128_CBC_SHA和TLS_DHE_RSA_WITH_AES_256_CBC_SHA。

在Firefox这些可以通过此步骤禁用：

1. 导航对大约：设置。
2. `security.ssl3.dhe`的搜索由于。
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应急方案。反而，管理员在SSL配置里修改本地或域组策略排除密码器。

为了通过`gpedit.msc Windows`模块修改本地策略，请导航到Computer Configuration >Administrative工具>Network >SSL配置设置>SSL密码器套件命令。

如果套件命令设置的已禁用或那么没配置默认顺序使用和对UCCX/Finesse的块访问。反而，应该设置这到已启用，并且应该修改密码器套件命令排除以上提到的两密码器。注释限制将使用密码器列表，因为他们不可以超出长度1023个字符。已知的密码器列表与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

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

此问题在UCCX 10.6(1) SU2或11.0不提交，木材堵塞漏洞在这些版本修复。有缺陷关联与此问题，[CSCuv89545](#)，在UCCX 10.6 SU1 ES02和SU2被解决。一个相关缺陷，[CSCuu82538](#)，在虚拟机运行红帽子企业6中被解决作为访客OS。

注意：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对版本10.6 SU2或删除KB更新