如何解决SSLv3在CVP的长卷毛狗弱点问题

目录

简介

此条款描述如何禁用安全套接字协议层版本3 (SSLv3)在Customer Voice Portal (CVP)为了解决在Downgraded传统加密(长卷毛狗)弱点问题的填充的Oracle。

贡献用纳塔利娅丰特斯丰特斯， Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- CVP服务器
- Cisco Unified Contact Center Enterprise (UCCE)
- 传输层安全(TLS)和其前身， SSL
- 互联网信息服务(IIS) Web服务器

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CVP 8.5(1)
- CVP 9.0(1)
- CVP 10.0(1)和10.5(1)

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。如果您的网络实际，请保证您了解所有命令的潜在影响。

问题

CVP能受长卷毛狗弱点的影响。

长卷毛狗是SSLv3协议弱点，并且允许攻击者对：

- 降级对版本SSLv3的SSL/TLS协议
- 中断口令安全

解决方案

Step1。从Windows Start菜单，请选择**启动> Control Panel > Administrative Tools > Services**。

选定服务：

- CVP CallServer
- Cisco CVP语音外部标记语言(VXML)服务器
- CVP操作控制台
- Cisco CVP WebServicesManager

点击**终止服务**链路在屏幕的左上角。

步骤2.备份位于路径的统一的CVP组件的server.xml文件。

- 呼叫服务器：

```
<Install drive:>\Cisco\CVP\CallServer\Tomcat\conf
```

- VXML服务器：

```
<install drive:>\Cisco\CVP\VXMLServer\Tomcat\conf
```

- WebServicesManager (WSM) ：

```
<install drive:>\Cisco\CVP\wsm\Server\Tomcat\conf
```

- 操作控制台(OAMP) ：

```
<install drive:>\Cisco\CVP\OPSConsoleServer\Tomcat\conf
```

第3.步。对于版本8.5， 9.0和10.0，在呼叫服务器，删除在server.xml文件的此线路：

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"/>
```

步骤4.修改在**server.xml文件的**连接器配置呼叫服务器、VXML服务器、WSM和OAMP的。

示例

```
<Connector SSLCertificateFile="C:\Cisco\CVP\conf\security\oamp.crt" SSLCertificateKeyFile=
"C:\Cisco\CVP\conf\security\oamp.key" SSLEnabled="true" acceptCount="100" clientAuth="false"
disableUploadTimeout="true" enableLookups="false" executor="tomcatThreadPool"
keyAlias="oamp_certificate"
keystoreFile="C:\Cisco\CVP\conf\security\.keystore"
keystorePass="F6.ov3Q@5rvd7r~7!AcDHtG1]c~5:$n"
keystoreType="JCEKS" maxHttpHeaderSize="8192" port="9443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
scheme="https" secure="true" sslProtocol="TLS" sslEnabledProtocols="TLSv1"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_
WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA"/>
```

步骤5.在IIS Web服务器的功能失效SSLv3。

在此位置创建子键：

```
<Connector SSLCertificateFile="C:\Cisco\CVP\conf\security\oamp.crt" SSLCertificateKeyFile=
"C:\Cisco\CVP\conf\security\oamp.key" SSLEnabled="true" acceptCount="100" clientAuth="false"
disableUploadTimeout="true" enableLookups="false" executor="tomcatThreadPool"
keyAlias="oamp_certificate"
keystoreFile="C:\Cisco\CVP\conf\security\.keystore"
keystorePass="F6.ov3Q@5rvd7r~7!AcDHtG1]c~5:$n"
keystoreType="JCEKS" maxHttpHeaderSize="8192" port="9443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
scheme="https" secure="true" sslProtocol="TLS" sslEnabledProtocols="TLSv1"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_
WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA"/>
```

设置这两把注册密匙：

```
<Connector SSLCertificateFile="C:\Cisco\CVP\conf\security\oamp.crt" SSLCertificateKeyFile=
"C:\Cisco\CVP\conf\security\oamp.key" SSLEnabled="true" acceptCount="100" clientAuth="false"
disableUploadTimeout="true" enableLookups="false" executor="tomcatThreadPool"
keyAlias="oamp_certificate"
keystoreFile="C:\Cisco\CVP\conf\security\.keystore"
keystorePass="F6.ov3Q@5rvd7r~7!AcDHtG1]c~5:$n"
keystoreType="JCEKS" maxHttpHeaderSize="8192" port="9443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
scheme="https" secure="true" sslProtocol="TLS" sslEnabledProtocols="TLSv1"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_
WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA"/>
```

第6.步。从Windows Start菜单，请选择**启动> Control Panel > Administrative Tools > Services**，并且重新启动这些服务。

- CVP CallServer
- Cisco CVP VXMLServer
- CVP操作控制台
- Cisco CVP WebServicesManager