Cómo resolver el problema de la vulnerabilidad del CANICHE SSLv3 en CVP

Contenido

Introducción

Este artículo describe cómo inhabilitar la versión 3 de Secure Sockets Layer (SSLv3) en el portal de la voz del cliente (CVP) para resolver el Oracle del acolchado en el problema de la vulnerabilidad del cifrado de la herencia Downgraded (CANICHE).

Contribuido por Natalia Fuentes Fuentes, ingeniero del TAC de Cisco.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servidor CVP
- Cisco Unified Contact Center Enterprise (UCCE)
- Transport Layer Security (TLS) y su precursor, SSL
- Servidor Web de los Servicios de Internet Information Server (IIS)

Componentes usados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Problema

CVP se podía afectar por la vulnerabilidad del CANICHE.

El CANICHE es una vulnerabilidad del protocolo SSLv3 y permite los atacantes a:

- Protocolo del Downgrade SSL/TLS a la versión SSLv3
- Rompa la seguridad criptográfica

Solución

Paso 1. Del menú Start (Inicio) de Windows, seleccione el **comienzo > el panel de control > > Services (Servicios) administrativo de las herramientas**.

Destaque los servicios:

- CVP CallServer
- Servidor externo del lenguaje de marcado de la Voz de Cisco CVP (VXML)
- Consola de las operaciones CVP
- Cisco CVP WebServicesManager

Parada del tecleo el link del **servicio** en la esquina superior izquierda de la pantalla.

Paso 2. Salvaguardia el fichero server.xml para los componentes unificados CVP situados en la trayectoria.

- Para el servidor de la llamada:

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

- Para el servidor VXML:

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

- Para WebServicesManager (WSM):

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

- Para la consola de las operaciones (OAMP):

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

Paso 3. Para las versiones 8.5, 9.0 y 10.0, en el servidor de la llamada, quitan esta línea en el fichero server.xml:

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

Paso 4. Modifique la configuración del conector en el **fichero server.xml** para el servidor de la llamada, el servidor VXML, el WSM, y OAMP.

Ejemplo:

```
<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"/>
```

Paso 5. Neutralización SSLv3 en el servidor Web IIS.

Cree un subkey en esta ubicación:

```
<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"/>
```

Fije estas dos claves de registro:

```
<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"/>
```

Paso 6. Del menú Start (Inicio) de Windows, seleccione el **comienzo > el panel de control > > Services (Servicios) administrativo de las herramientas**, y recomience estos servicios.

- CVP CallServer
- Cisco CVP VXMLServer
- Consola de las operaciones CVP
- Cisco CVP WebServicesManager