CVP の SSLv3 プードル脆弱性に関する 問題を解決する方法

目次

概要

この記事は Downgraded レガシー暗号化（プードル）脆弱性に関する 問題のパッディング Oracle を解決するために Cisco Unified Customer Voice Portal （CVP）の Secure Sockets Layer バージョン 3 （SSLv3）を無効に する方法を記述します。

ナタリア フェンテス フェンテスによって貢献される、Cisco TAC エンジニア。

前提条件

要件

次の項目に関する知識が推奨されます。

- CVP Server
- Cisco Unified Contact Center Enterprise（UCCE）
- Transport Layer Security （TLS）および先行処理、SSL
- Internet Information Services （IIS） Webサーバ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- CVP 8.5(1)

- CVP 9.0(1)
- CVP 10.0(1) および 10.5(1)

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

問題

CVP はプードル脆弱性から影響を受けることができます。

プードルは SSLv3 プロトコル脆弱性であり、攻撃者をに可能にします:

- バージョン SSLv3 へのダウングレード SSL/TLS プロトコル
- 暗号セキュリティを壊して下さい

解決策

ステップ 1： Windows Start メニューから、**> 管理上の Tools > Services** Start > Control Panel の順に選択 して下さい。

サービスをハイライト表示して下さい:

- CVP CallServer
- Cisco CVP 音声外部マークアップ言語（VXML）サーバ
- CVP オペレーション コンソール
- Cisco CVP WebServicesManager

画面の左上のコーナーの**サービス** リンクを『Stop』 をクリック して下さい。

ステップ 2.パスで取付けられる統一された CVP コンポーネントのための server.xml ファイルをバックアップして下さい。

- コール サーバに関しては:

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

- VXML サーバに関しては:

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

- WebServicesManager （WSM）に関しては:

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

- オペレーション コンソール（OAMP）に関しては:

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

ステップ 3 バージョン 8.5 に関しては、9.0 および 10.0 は、コール サーバで、server.xml ファイルのこのラインを削除します:

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

ステップ 4.コール サーバ、VXML サーバ、WSM および OAMP のための server.xml ファイルのコネクタ 設定を修正して下さい。

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"/>
```

ステップ 5. IIS Webサーバの無効 SSLv3。

この場所のサブ キーを作成して下さい:

```
<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"/>
```

これら二つのレジストリキーを設定 して下さい:

```
<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"/>
```

ステップ 6 Windows Start メニューから、**> 管理上の Tools > Services** Start > Control Panel の順に選択 し、これらのサービスを再開して下さい。

- CVP CallServer
- Cisco CVP VXMLServer
- CVP オペレーション コンソール
- Cisco CVP WebServicesManager