Permita a característica de configuração cifrada no CUCM

Índice

Introdução

Este documento descreve o uso de arquivos cifrados do telefone da configuração no gerente das comunicações unificadas de Cisco (CUCM).

Informações de Apoio

O uso de arquivos de configuração cifrados para telefones é uns recursos de segurança opcionais que estejam disponíveis no CUCM.

Você não é exigido executar o conjunto CUCM em modo misturado para que esta característica funcione corretamente, porque a informação do certificado da função do proxy do Certificate Authority (CAPF) é contida dentro do arquivo da lista da confiança da identidade (ITL).

> **Note**: Este é o local padrão para todas as versões 8.X e mais recente CUCM. Para versões CUCM antes da versão 8.X, você deve assegurar-se de que o conjunto seja executado em modo misturado se você deseja usar esta característica.

Visão geral de características cifrada da configuração

Esta seção descreve o processo que ocorre quando os arquivos cifrados do telefone da configuração são usados dentro do CUCM.

Quando você permite esta característica, restaura o telefone, e transfere o arquivo de configuração, você recebe um pedido para o arquivo com uma **extensão .cnf.xml.sgn:**

Contudo, depois que a característica de configuração cifrada é permitida no CUCM, o serviço TFTP já não gerencie um arquivo de configuração direta com a **extensão .cnf.xml.sgn.** Em lugar de, gerencie o arquivo de configuração parcial, segundo as indicações do exemplo seguinte.

Note: Quando você usa este método pela primeira vez, o telefone compara a mistura MD5 do certificado do telefone no arquivo de configuração à mistura MD5 localmente - do certificado significativo (LSC) ou dos Certificados instalados fabricação (MIC).

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
<certHash></certHash>
<encrConfig>true</encrConfig>
</device>
```

Se o telefone identifica um problema, tenta iniciar uma sessão com o CAPF, a menos que o modo de autenticação CAPF combinar por *string de autenticação*, neste caso você deve manualmente entrar na corda. Estão aqui alguns problemas que o telefone pôde identificar:

- A mistura não combina.
- O telefone não contém um certificado.
- O valor MD5 está vazio (como no exemplo anterior).

Note: O telefone inicia uma sessão do Transport Layer Security (TLS) ao serviço CAPF na porta 3804 à revelia.

O certificado CAPF deve ser sabido para o telefone, assim que deve ser incluído no arquivo ITL ou no arquivo do certificate trust list (CTL) (se o conjunto é executado em modo misturado).

Depois que a comunicação CAPF é estabelecida, o telefone envia a informação ao CAPF sobre o LSC ou o MIC que é usado. O CAPF então extrai a chave pública do telefone do LSC ou do MIC, gerencie uma mistura MD5, e armazena os valores para a chave pública e a mistura do certificado no base de dados CUCM.

```
admin:run sql select md5hash,name from device where name='SEPA45630BBFA40'
md5hash name
================================ ===============
6e566143c1c14566c9da943d949a79c8 SEPA45630BBFA40
```

Depois que a chave pública é armazenada no base de dados, o telefone restaura e pede um arquivo de configuração novo. O telefone tenta transferir **mais uma vez o** arquivo de configuração com a **extensão cnf.xml.sgn**.

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
```

```
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
<certHash>6e566143c1c14566c9da943d949a79c8</certHash>
<encrConfig>true</encrConfig>
</device>
```

O telefone compara o **cerHash** outra vez, e se não detecta o problema, transfere o arquivo de configuração cifrado com a **extensão .cnf.xml.enc.sgn.**

```
............c..)CN=cucm85;OU=It;O=Cisco;L=KRK;ST=PL;C=PL....Z.........)CN=cucm85;
OU=It;O=Cisco;L=KRK;ST=PL;C=PL...........
..........C.<...Y6.Lh.|(..w+..,.0.a.&.
O..........V....T...Z..R^..f....|.=.e.@...5...........G...[.........n.........=
.A..H.(....Z...{.!%[.. SEPA45630BBFA40.cnf.xml.enc.sgn....R.DD..M............
Uu.C..@...........
...................m.b.......6y ..x.^b..-8.^..^'.4.<Wb.n.....5...we.0@..g..
V7.,..r.9
Qs>..).w....pt/...}A.']
.r.t%G..d_.;u.rEI.pr.F
.....M..r...o.N
.=..g.^P....Pz....J..E.S...d|Z).....J..&..I....7.r..g8.{f..o.....:.~..U...5G+V.
[...]
```

Permita a característica de configuração cifrada

A fim permitir os arquivos cifrados do telefone da configuração, você deve criar (ou para editar uma corrente) um perfil de segurança novo do telefone e atribui-lo ao telefone. Termine estas etapas a fim permitir a característica de configuração cifrada no CUCM:

1. O log na página de administração CUCM e navega ao **> segurança do sistema > ao perfil de segurança do telefone**:

2. Copie uma corrente, ou crie um novo, telefone ao perfil de segurança e verifique a caixa de verificação **cifrada TFTP da configuração**:

3. Atribua o perfil ao telefone:

Troubleshooting

Termine estas etapas a fim pesquisar defeitos edições do sistema com respeito à característica de configuração cifrada:

1. Assegure-se de que o serviço CAPF esteja ativo e seja executado corretamente no nó do editor no conjunto CUCM.

2. Transfira o arquivo de configuração parcial e verifique que a porta e o endereço IP de Um ou Mais Servidores Cisco ICM NT do serviço CAPF são alcançáveis do telefone.

3. Verifique a comunicação TCP na porta 3804 ao nó do editor.

4. Execute o comando previamente mencionado da língua de consulta estruturada (SQL) a fim verificar se o serviço CAPF tem a informação sobre o LSC ou o MIC que é usado pelo telefone.

5. Se a edição ainda persiste, você pôde ser exigido recolher a informação adicional do sistema. Reinicie o telefone e recolha esta informação:

   Telefone a logs do consoleLogs de Cisco TFTPLogs de Cisco CAPFCapturas de pacote de informação do CUCM e do telefone

Refira estes recursos para obter informações adicionais sobre de como executar capturas de pacote de informação do CUCM e do telefone:

- Recolhendo traços CUCM de CUCM 8.6.2 para um SÊNIOR TAC
- Captura de pacote de informação no modelo do dispositivo do gerente das comunicações unificadas
- Recolhendo uma captura de pacote de informação de um Cisco IP Phone

Nos logs e nas capturas de pacote de informação, você deve assegurar-se de que o processo descrito nas seções anterior funcione corretamente. Especificamente, verifique isso:

- O telefone transfere o arquivo de configuração parcial com a informação correta CAPF.
- O telefone conecta através do TLS ao serviço CAPF, e aquele a informação sobre o LSC ou o MIC é atualizado no base de dados.
- O telefone transfere o arquivo de configuração cifrado completo.