Diretório corporativo do “edições não encontradas host”

ID do Documento: 118699

Atualizado em: janeiro 26, 2015

Contribuído por Gagarin Sathiyanarayanan, engenheiro de TAC da Cisco.

Produtos Relacionados

- Cisco Unified Communications Manager (CallManager)

Índice

Introdução

Este documento descreve como pesquisar defeitos do “edições não encontradas host” no diretório corporativo. A informação importante relevante a este documento é:

- O diretório corporativo é Cisco-forneceu o serviço de telefone do IP padrão que instala automaticamente com o gerente das comunicações unificadas de Cisco (CUCM).
- A tabela de “TelecasterService” armazena os parâmetros para todos os serviços de telefone que são fornecida no sistema.
- No telefone quando você seleciona a opção “diretório corporativo”, o telefone envia um pedido HTTP ou HTTPS a um dos server CUCM e é retornado um objeto XML como uma resposta HTTP.

Informações importantes

- Esclareça se a edição ocorre quando você alcançar “diretórios” ou “diretório corporativo”.
- Que é do “o conjunto de campo serviço URL” sob ao serviço de diretório corporativo? Se a URL é ajustada ao “aplicativo: Cisco/CorporateDirectory” então, com base na versão de firmware do telefone, o telefone faz um pedido HTTP ou HTTPS.Os telefones que usam a versão de firmware 9.3.3 e mais atrasado à revelia fazem um pedido HTTPS.
- Quando o serviço URL for ajustado ao “aplicativo: Cisco/CorporateDirectory”, o telefone envia o pedido do HTTP ao server que é primeiro nele é grupo do CallManager (CM).
- Identifique a topologia de rede entre o telefone e o server a que o pedido do HTTP é enviado.
- Pague a atenção aos Firewall, optimizers MACILENTOS, e assim por diante no trajeto que pode deixar cair/tráfego de HTTP do cabaz.

Encenação de trabalho

Nesta encenação, o serviço de telefone URL é ajustado ao “aplicativo: Cisco/CorporateDirectory” e os usos HTTPS do telefone.

Este exemplo mostra o arquivo de configuração do telefone com a URL correta.

```
<phoneService  type="1" category="0">
<name>Corporate Directory</name>
<url>Application:Cisco/CorporateDirectory</url>
<vendor></vendor>
<version></version>
</phoneService>
```

Dos logs do console do telefone você poderá verificar estas etapas.

1. O telefone usa o HTTPS URL.`7949 NOT 11:04:14.765155  CVM-appLaunchRequest: [thread=AWT-EventQueue-0]`
   `[class=cip.app.G4ApplicationManager] Creating application module - Corporate Directory`
   `7950 ERR 11:04:14.825312 CVM-XsiAppData&colon;:getCdUrl:`
   `[thread=appmgr MQThread]`
   `[class=cip.app.ar] Using HTTPS URL`
2. O certificado da Web de Tomcat apresentado ao telefone do server dos diretórios não estará disponível no telefone. Daqui o telefone tenta autenticar o certificado através do serviço da verificação da confiança (TV).`7989 ERR 11:04:15.038637  SECD: -HTTPS cert not in CTL, <10.106.111.100:8443>`
   `7990 NOT 11:04:15.038714 SECD: -TVS service available, will attempt via TVS`
3. Os olhares do telefone no theTVS põem em esconderijo primeiramente e se não encontraram que contacta o server TV.`7995 NOT 11:04:15.039286  SECD: -TVS Certificate Authentication request`
   `7996 NOT 11:04:15.039394 SECD: -No matching entry found at cache`
4. Desde que a conexão ao theTVS é igualmente segura, um certificado de autenticação está terminado e esta mensagem é imprimida se é bem sucedida.`8096 NOT 11:04:15.173585  SECD: -Successfully obtained a TLS connection to the TVS server`
5. O telefone envia agora um pedido autenticar o certificado.`8159 NOT 11:04:15.219065  SECD: -Successfully sent the certificate Authentication request to TVS server, bytes written : 962`
   `8160 NOT 11:04:15.219141 SECD: -Done sending Certificate Validation request`
   `8161 NOT 11:04:15.219218 SECD: -Authenticate Certificate : request sent to`

```
TVS server - waiting for response
```

6. A resposta "0" dos TV significa que a autenticação era bem sucedida. `8172 NOT 11:04:15.220060  SECD: -Authentication Response received, status : 0`
7. Esta mensagem é indicada e então você verá a resposta.`8185 NOT 11:04:15.221043  SECD: -Authenticated the HTTPS conn via TVS`

```
8198 NOT 11:04:15.296173 CVM-[truncated] Received
HTTP/1.1 200 OK^M
X-Frame-Options: SAMEORIGIN^M
Set-Cookie: JSESSIONID=660646D3655BB00734D3895606BCE76F;
Path=/ccmcip/; Secure; HttpOnly^M
Content-Type: text/xml;charset=utf-8^M
Content-Length: 966^M
Date: Tue, 30 Sep 2014 11:04:15 GMT^M
Server: ^M
^M
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><CiscoIPPhoneInput>
<Title>Directory Search</Title><Prompt>Enter search criteria</Prompt><SoftKeyItem>
<Name>Search</Name><Position>1</Position><URL>SoftKey:Submit</URL></SoftKeyItem>
<SoftKeyItem><Name>&lt;&lt;</Name><Position>2</Position><URL>SoftKey:&lt;&lt;</URL>
</SoftKeyItem><SoftKeyItem><Name>Cancel</Name><Position>3</Position>
<URL>SoftKey:Cancel</URL></SoftKeyItem>
<URL>https://10.106.111.100:8443/ccmcip/xmldirectorylist.jsp</URL>
<InputItem><DisplayName>First Name</DisplayName>
<QueryStringParam>f</QueryStringParam><InputFlags>A</InputFlags>
<DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Last Name</DisplayName><QueryStringParam>l</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
```

`<DisplayName>`O processo de certificado de autenticação é similar ao que é discutido no serviço da verificação da confiança dos contatos do telefone para certificado desconhecido.Das capturas de pacote de informação (PCAPs) recolhidas na extremidade do telefone, você deve poder verificar a comunicação TV com o uso deste filtro - "tcp.port==2445".

Nos logs simultâneos TV:

1. A revisão segue com respeito à agitação da mão do Transport Layer Security (TLS).
2. Em seguida, reveja a cópia parcial da memória de HEX entrante.`04:04:15.270 |  debug ipAddrStr (Phone) 10.106.111.121`

```
04:04:15.270 |<--debug
04:04:15.270 |-->debug
04:04:15.270 | debug 2:UNKNOWN:Incoming Phone Msg:
.
.
04:04:15.270 | debug
HEX_DUMP: Len = 960:

04:04:15.270 |<--debug
04:04:15.270 |-->debug
04:04:15.270 | debug 57 01 01 00 00 00 03 ea
.
<<o/p omitted >>
.
04:04:15.271 | debug MsgType : TVS_MSG_CERT_VERIFICATION_REQ
```

3. Os TV recuperam os detalhes do expedidor.`04:04:15.272 |-->CDefaultCertificateReader::GetIssuerName`

```
04:04:15.272 | CDefaultCertificateReader::GetIssuerName got issuer name
04:04:15.272 |<--CDefaultCertificateReader::GetIssuerName
04:04:15.272 |-->debug
04:04:15.272 | debug tvsGetIssuerNameFromX509 - issuerName :
CN=cucm10;OU=TAC;O=Cisco;L=Blore;ST=KN;C=IN and Length: 43
```

```
04:04:15.272 |<--debug
```

4. Os TV verificam o certificado.
```
04:04:15.272 |   debug tvsGetSerialNumberFromX509 -
serialNumber :
6F969D5B784D0448980F7557A90A6344 and Length: 16
04:04:15.272 | debug CertificateDBCache::getCertificateInformation -
Looking up the certificate cache using Unique MAP ID :
6F969D5B784D0448980F7557A90A6344CN=cucm10;OU=TAC;O=Cisco;L=Blore;ST=KN;C=IN
04:04:15.272 | debug CertificateDBCache::getCertificateInformation -
Certificate compare return =0
04:04:15.272 | debug CertificateDBCache::getCertificateInformation -
Certificate found and equal
```

5. Os TV enviam a resposta ao telefone.
```
04:04:15.272 |   debug 2:UNKNOWN:Sending
CERT_VERIF_RES msg
04:04:15.272 | debug MsgType : TVS_MSG_CERT_VERIFICATION_RES
```

O serviço de telefone URL é ajustado ao “aplicativo: Cisco/CorporateDirectory” e os usos HTTP do telefone

> Nota: Em vez do uso de uma versão de firmware mais adiantada do telefone, o serviço e o serviço seguro URL duro-foram codificados ao URL DO HTTP. Contudo, a mesma sequência de evento é considerada no firmware do telefone que utiliza o HTTP à revelia.

O arquivo de configuração do telefone tem a URL correta.

```
<phoneService  type="1" category="0">
<name>Corporate Directory</name>
<url>Application:Cisco/CorporateDirectory</url>
<vendor></vendor>
<version></version>
</phoneService>
```

Dos logs do console do telefone você poderá verificar estas etapas.

```
7250 NOT 11:44:49.981390  CVM-appLaunchRequest: [thread=AWT-EventQueue-0]
[class=cip.app.G4ApplicationManager] Creating application module -
Corporate Directory/-838075552
7254 NOT 11:44:50.061552 CVM-_HTTPMakeRequest1: Processing Non-HTTPS URL
7256 NOT 11:44:50.061812 CVM-_HTTPMakeRequest1() theHostname: 10.106.111.100:8080


7265 NOT 11:44:50.233788 CVM-[truncated] Received
HTTP/1.1 200 OK^M
X-Frame-Options: SAMEORIGIN^M
Set-Cookie: JSESSIONID=85078CC96EE59CA822CD607DDAB28C91;
Path=/ccmcip/; HttpOnly^M
Content-Type: text/xml;charset=utf-8^M
Content-Length: 965^M
Date: Tue, 30 Sep 2014 11:44:50 GMT^M
Server: ^M
^M
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><CiscoIPPhoneInput>
<Title>Directory Search</Title><Prompt>Enter search criteria</Prompt><SoftKeyItem>
<Name>Search</Name><Position>1</Position><URL>SoftKey:Submit</URL></SoftKeyItem>
<SoftKeyItem><Name>&lt;&lt;</Name><Position>2</Position><URL>SoftKey:&lt;&lt;</URL>
</SoftKeyItem><SoftKeyItem><Name>Cancel</Name><Position>3</Position>
<URL>SoftKey:Cancel</URL></SoftKeyItem>
<URL>http://10.106.111.100:8080/ccmcip/xmldirectorylist.jsp</URL><InputItem>
<DisplayName>First Name</DisplayName><QueryStringParam>f</QueryStringParam>
```

```
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Last Name</DisplayName><QueryStringParam>l</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Number</D
```

Das capturas de pacote de informação você verá um pedido HTTP GET e uma RESPOSTA bem sucedida. Este é o PCAP de CUCM:

Troubleshooting

Antes que você pesquise defeitos, recolha os detalhes da edição alistada mais cedo:

Logs a recolher, se for necessário

- Capturas de pacote de informação simultâneas do telefone IP e do server CUCM (o server que é primeiro nele é o grupo CM a onde o pedido do HTTP seria enviado).
- Logs do console do telefone IP.
- Logs de Cisco TV (detalhados).Quando você ajusta os logs TV a detalhado, o serviço precisa de ser reiniciado para que as mudanças do nível de rastreamento ocorram. Veja a identificação de bug Cisco CSCuq22327 para o realce para notificar que um reinício do serviço está exigido quando os níveis do log são mudados.

Termine estas etapas a fim isolar a edição:

Passo 1

Crie um serviço do teste com estes detalhes:

```
Service Name : <Any Name>
Service URL : http://<CUCM_IP_Address>:8080/ccmcip/xmldirectoryinput.jsp
Secure-Service URL : http://<CUCM_IP_Address>:8080/ccmcip/xmldirectoryinput.jsp
Service Category : XML Service
Service Type : Directories
Enable : CHECK
Enterprise Subscription : DO NOT CHECK
```

Agora, subscreva este serviço a um dos telefones afetados:

1. Vá à página da configuração de dispositivo.
2. Seleto **subscreva/serviços do cancelar assinatura** sob os links relacionados.
3. Subscreva o serviço que do teste você criou.
4. Salvar, aplique a configuração, e restaure o telefone. O que você fez é, independentemente da versão FW do telefone que determina se usar o HTTP ou o HTTPS URL, o força para usar o URL DO HTTP.Alcance o serviço do “diretório corporativo” no telefone.Se não trabalha, a seguir para recolher os logs mencionados acima e para compará-los com a encenação de trabalho mencionada sob “a encenação de trabalho” e para identificar onde o desvio está.Se trabalha, a seguir você confirmou pelo menos que da perspectiva do serviço de telefone IP CUCM não há nenhuma edição.Nesta fase a edição poderia o mais provavelmente ser com os telefones que usam o HTTPS URL.Agora, escolha um telefone que não funcione e continue à próxima etapa.

Quando trabalha com esta mudança, você precisa de decidir se é APROVADO deixar a configuração com o pedido/resposta do diretório corporativo que trabalha sobre o HTTP em vez do HTTPS. Uma comunicação HTTPS não trabalha devido a uma das razões discutiu em

seguida.

Passo 2

Recolha os logs mencionados previamente e compare-os com a encenação de trabalho mencionada sob “a encenação de trabalho” e identifique-o onde o desvio está.

Poderia ser uma destas edições:

1. O telefone é incapaz de contactar o server TV. No PCAPS, verifique a comunicação na porta 2445.Assegure-se de que nenhuns dos dispositivos de rede no bloco do trajeto esta porta.
2. O telefone contacta o server TV, mas o handshake de TLS falha.Estas linhas serão imprimidas nos logs do console do telefone:`5007: NOT 10:25:10.060663 SECD: clpSetupSsl: Trying to connect to IPV4, IP: 192.168.136.6, Port : 2445 5008: NOT 10:25:10.062376 SECD: clpSetupSsl: TCP connect() waiting, <192.168.136.6> c:14 s:15 port: 2445 5009: NOT 10:25:10.063483 SECD: clpSetupSsl: TCP connected, <192.168.136.6> c:14 s:15 5010: NOT 10:25:10.064376 SECD: clpSetupSsl: start SSL/TLS handshake, <192.168.136.6> c:14 s:15 5011: ERR 10:25:10.068387 SECD: EROR:clpState: SSL3 alert read:fatal:handshake failure:<192.168.136.6> 5012: ERR 10:25:10.069449 SECD: EROR:clpState: SSL_connect:failed in SSLv3 read server hello A:<192.168.136.6> 5013: ERR 10:25:10.075656 SECD: EROR:clpSetupSsl: ** SSL handshake failed, <192.168.136.6> c:14 s:15 5014: ERR 10:25:10.076664 SECD: EROR:clpSetupSsl: SSL/TLS handshake failed, <192.168.136.6> c:14 s:15 5015: ERR 10:25:10.077808 SECD: EROR:clpSetupSsl: SSL/TLS setup failed, <192.168.136.6> c:14 s:15 5016: ERR 10:25:10.078771 SECD: EROR:clpSndStatus: SSL CLNT ERR, srvr<192.168.136.6>`Veja a identificação de bug Cisco CSCua65618 para mais informação.
3. O telefone contacta os server TV e o handshake de TLS é bem sucedido, mas os TV são incapazes de verificar o signatário do certificado que o telefone pedido autenticar.Os snippet dos logs TV são alistados aqui:O telefone contacta os TV.

`05:54:47.779 | debug 7:UNKNOWN:Got a new ph conn 10.106.111.121 on 10, Total Acc = 6.. . .`
`05:54:47.835 | debug MsgType : TVS_MSG_CERT_VERIFICATION_REQ`Os TV obtêm o nome de emissor.`05:54:47.836 |-->CDefaultCertificateReader::GetIssuerName 05:54:47.836 | CDefaultCertificateReader::GetIssuerName got issuer name 05:54:47.836 |<--CDefaultCertificateReader::GetIssuerName 05:54:47.836 |-->debug 05:54:47.836 | debug tvsGetIssuerNameFromX509 - issuerName : CN=cucmpub9;OU=TAC;O=Cisco;L=Bangalore;ST=KN;C=IN and Length: 49`Olha acima o certificado, mas não pode encontrá-lo.`05:54:47.836 | debug CertificateCTLCache::getCertificateInformation - Looking up the certificate cache using Unique MAP ID : 62E09123B09A61D20E77BE5BF5A82CD4CN=cucmpub9;OU=TAC;O=Cisco;L=Bangalore;ST=KN;C=IN 05:54:47.836 |<--debug 05:54:47.836 |-->debug 05:54:47.836 | debug ERROR:CertificateCTLCache::getCertificateInformation - Cannot find the certificate in the cache 05:54:47.836 |<--debug`

```
05:54:47.836 |-->debug
05:54:47.836 | debug getCertificateInformation(cert) : certificate not found
```

4. O tráfego HTTPS é obstruído/deixado cair em algum lugar na rede.Consiga PCAPs simultâneo do telefone e do server CUCM a fim verificar a comunicação.

Outras encenações quando do “a edição não encontrada host” ocorrer

1. O server CUCM é definido pelo hostname junto com edições na resolução de nome.
2. A lista de servidor TV está vazia no telefone quando transfere o arquivo xmldefault.cnf.xml. (Na versão 8.6.2 o arquivo de configuração padrão não terá a entrada TV nele devido à identificação de bug Cisco CSCti64589.)
3. O telefone é incapaz de usar a entrada TV no arquivo de configuração porque transferiu o arquivo xmldefault.cnf.xml. Veja a identificação de bug Cisco CSCuq33297 - Phoneto analisa gramaticalmente a informação TV do arquivo de configuração padrão.
4. O diretório corporativo não trabalha após uma elevação CUCM porque as upgrades de firmware do telefone a uma versão mais atrasada que mude eventualmente o comportamento do uso do HTTPS à revelia.

Cisco relacionado apoia discussões da comunidade

Atualizado em: janeiro 26, 2015
ID do Documento: 118699