Seguridad CUCM por abandono y operación y troubleshooting ITL

Contenido

Introducción

Este documento describe la característica de la Seguridad por abandono (SBD) de las versiones 8.0 del administrador de las Comunicaciones unificadas de Cisco (CUCM) y posterior. Este documento sirve como suplemento a los documentos oficiales de la Seguridad por abandono, y proporciona la información de funcionamiento y los consejos de Troubleshooting para ayudar a los administradores y para facilitar el proceso de Troubleshooting.

Antecedentes

La versión 8.0 y posterior CUCM introduce la característica SBD, que consiste en los archivos y el servicio de la verificación de la confianza (TV) de la lista de la confianza de la identidad (ITL).

Cada cluster CUCM ahora utiliza la Seguridad ITL-basada automáticamente. Hay un equilibrio entre la Seguridad y la facilidad de empleo/la facilidad de la administración de la cual los administradores deben ser conscientes antes de que realicen ciertos cambios a una versión 8.0 CUCM agrupar.

Es una buena idea llegar a ser familiar con estos conceptos de la base de SBD: Artículo dominante asimétrico de Wikipedia del artículo y del Public Key Infrastructure de Wikipedia de la criptografía.

Descripción SBD

Esta sección proporciona una descripción rápida de exactamente qué el SBD proporciona. Para los detalles técnicos completos de cada función, vea el SBD sección detallar y de información de Troubleshooting.

El SBD proporciona estas tres funciones para los Teléfonos IP soportados:

- Autenticación predeterminada de los archivos descargados TFTP (configuración, escena, ringlist) ese uso una clave de firma
- Cifrado opcional de los archivos de configuración de TFTP que utilizan una clave de firma
- Verificación del certificado para las conexiones HTTPS teléfono-iniciadas que utilizan un almacén remoto de la confianza del certificado en CUCM (TV)

Este documento proporciona una descripción de cada uno de estas funciones.

Autenticación de la descarga TFTP

Cuando a Certificate Trust List (Lista de confianza del certificado) (CTL) o el archivo ITL está presente, el teléfono del IP pide un archivo de configuración de TFTP firmado del servidor TFTP CUCM. Este archivo permite que el teléfono verifique que el archivo de configuración viniera de una fuente confiable. Con los archivos CTL/ITL presentes en los teléfonos, los archivos de configuración se deben firmar por un servidor TFTP de confianza. El archivo es sólo texto en la red mientras que se transmite, pero viene con una firma especial de la verificación.

El teléfono pide **SEP *< la dirección MAC >.cnf.xml.sgn* para** recibir el archivo de configuración con la firma especial. Este archivo de configuración es firmado por la clave privada TFTP que corresponde a CallManager.pem en la página de la administración de certificados de la administración del operating system (OS).

El archivo firmado tiene una firma en el superior para autenticar el archivo, pero está de otra manera en el sólo texto XML. La imagen abajo muestra que el firmante del archivo de configuración es **CN=CUCM8-Publisher.bbbburns.lab** cuál a su vez es firmado por **CN=JASBURNS-AD**. Esto significa que el teléfono necesita verificar la firma de **CUCM8-Publisher.bbbburns.lab** contra el archivo ITL antes de que se valide este archivo de configuración.

Aquí está un diagrama que muestra cómo la clave privada se utiliza junto con un algoritmo condensado de mensaje (MD)5 o algoritmo de troceo seguro (función de troceo SHA)1 para crear el archivo firmado.

La verificación de firma invierte este proceso con el uso de la clave pública que las coincidencias

para desencriptar el hash. Si desmenuza la coincidencia, muestra:

- Este archivo no se ha modificado adentro transita.
- Este archivo viene del partido enumerado en la firma, puesto que cualquier cosa desencriptada con éxito con la clave pública se debe haber cifrado con la clave privada.

Cifrado del archivo de configuración de TFTP

Si el cifrado opcional de la configuración de TFTP se habilita en el perfil de seguridad asociado del teléfono, el teléfono pide un archivo de configuración cifrado. Este archivo se firma con la clave privada TFTP y se cifra con una clave simétrica intercambiada entre el teléfono y el CUCM (refiera a la guía de la Seguridad del administrador de las Comunicaciones unificadas de Cisco, liberan 8.5(1) para las profundidades totales) para no poder leer su contenido con un sabueso de red a menos que el observador tenga las claves necesarias.

El teléfono pide **SEP** *< la dirección MAC >.cnf.xml.enc.sgn* **para** conseguir el archivo cifrado firmado.

El archivo de configuración cifrado tiene la firma al principio también, pero no hay datos del sólo texto después de, sólo los datos encriptados (caracteres binarios mutilados en este editor de textos). La imagen muestra que el firmante es lo mismo que en el ejemplo anterior, así que este firmante debe estar presente en el archivo ITL antes de que el teléfono valide el archivo. Además, las claves del desciframiento deben estar correctas antes de que el teléfono pueda leer el contenido del archivo.

Servicio de la verificación de la confianza (verificación remota del certificado y de firma)

Los Teléfonos IP contienen las cantidades limitadas de memoria, y puede también haber un gran número de teléfonos a manejar en una red. CUCM actúa como almacén remoto de la confianza vía los TV para no tener que colocar un almacén lleno de la confianza del certificado en cada teléfono del IP. Cualquier momento el teléfono no puede verificar una firma o un certificado vía los archivos CTL o ITL, pregunta a servidor para verificación TV. Este almacén central de la confianza es más fácil de manejar que si el almacén de la confianza estaba presente en todos los Teléfonos IP.

Detalle y información de Troubleshooting SBD

Esta sección detalla el proceso SBD.

Archivos y Certificados ITL presentes en CUCM

Primero, hay varios archivos que deben estar presentes en el servidor sí mismo CUCM. El pedazo más importante es el certificado TFTP y la clave privada TFTP. El certificado TFTP está situado bajo el **Certificate Management (Administración de certificados) del > Security (Seguridad) de la administración OS > CallManager.pem.**

El servidor CUCM utiliza el soldado y las claves públicas del certificado CallManager.pem para servicio TFTP (así como para el servicio del Cisco Call Manager (CCM)). La imagen muestra que el certificado CallManager.pem está publicado a CUCM8-publisher.bbbburns.laband **firmado** por JASBURNS-AD**. Todos los** archivos de configuración de TFTP son firmados por la clave privada abajo.

Todos los teléfonos pueden utilizar la clave pública TFTP en el certificado CallManager.pem para desencriptar cualquier archivo cifrado con la clave privada TFTP, así como verificar cualquier archivo firmado con la clave privada TFTP.

Además de la clave privada del certificado CallManager.pem, el servidor CUCM también salva un archivo ITL que se presente a los teléfonos. **El comando del** showitl muestra los contenidos totales de este archivo ITL vía el acceso del Secure Shell (SSH) al servidor OS CLI CUCM.

Esta sección analiza el archivo ITL pieza por pieza, porque tiene varios componentes importantes que el teléfono utilice.

La primera porción es la información de firma. Incluso el archivo ITL es un archivo firmado. Esta salida muestra que es firmada por la clave privada TFTP que se asocia al certificado anterior CallManager.pem.

```
admin:show itl
Length of ITL file: 5438
The ITL File was last modified on Wed Jul 27 10:16:24 EDT 2011

       Parse ITL File
       ----------------

Version:        1.2
HeaderLength:   296 (BYTES)

BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
3       SIGNERID        2       110
4       SIGNERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
5       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:00:05
6       CANAME          15      CN=JASBURNS-AD
*Signature omitted for brevity*
```

Las siguientes secciones cada uno contienen su propósito dentro de un parámetro de la función especial. La primera función es el token de seguridad del administrador de sistema. Ésta es la firma de la clave pública TFTP.

```
        ITL Record #:1
                 ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1972
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       System Administrator Security Token
5       ISSUERNAME      15      CN=JASBURNS-AD
6       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:00:05
7       PUBLICKEY       140
8       SIGNATURE       256
9       CERTIFICATE     1442    0E 1E 28 0E 5B 5D CC 7A 20 29 61 F5
                                8A DE 30 40 51 5B C4 89 (SHA1 Hash HEX)
```

```
This etoken was used to sign the ITL file.
```

La función siguiente es CCM+TFTP. Ésta es otra vez la clave pública TFTP que sirve autenticar y desencriptar los archivos de configuración de TFTP descargados.

```
        ITL Record #:2
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1972
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      15      CN=JASBURNS-AD
6       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:00:05
7       PUBLICKEY       140
8       SIGNATURE       256
9       CERTIFICATE     1442    0E 1E 28 0E 5B 5D CC 7A 20 29 61 F5
                                8A DE 30 40 51 5B C4 89 (SHA1 Hash HEX)
```

La función siguiente es TV. Hay una entrada para la clave pública de cada servidor TV con la cual el teléfono conecta. Esto permite que el teléfono establezca una sesión de Secure Sockets Layer (SSL) al servidor TV.

```
        ITL Record #:3
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       743
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       TVS
5       ISSUERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       2E:3E:1A:7B:DA:A6:4D:84
7       PUBLICKEY       270
8       SIGNATURE       256
11      CERTHASH        20      C7 E1 D9 7A CC B0 2B C2 A8 B2 90 FB
                                AA FE 66 5B EC 41 42 5D
12      HASH ALGORITHM  1       SHA-1
```

La función final incluida en el archivo ITL es la función de proxy del Certificate Authority (CAPF). Este certificado permite que los teléfonos establezcan una conexión segura al servicio del CAPF en el servidor CUCM de modo que el teléfono pueda instalar o poner al día a localmente - el certificado significativo (LSC). Este proceso será cubierto en otro documento que deba todavía ser liberado.

```
        ITL Record #:4
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       455
2       DNSNAME         2
3       SUBJECTNAME     61      CN=CAPF-9c4cba7d;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       CAPF
5       ISSUERNAME      61      CN=CAPF-9c4cba7d;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       0A:DC:6E:77:42:91:4A:53
7       PUBLICKEY       140
8       SIGNATURE       128
11      CERTHASH        20      C7 3D EA 77 94 5E 06 14 D2 90 B1
```

```
                              A1 43 7B 69 84 1D 2D 85 2E
12      HASH ALGORITHM  1     SHA-1

The ITL file was verified successfully.
```

Las cubiertas de la siguiente sección exactamente qué sucede cuando un teléfono inicia.

El teléfono descarga la ITL y el archivo de configuración

Después de que el teléfono inicie y obtenga una dirección IP así como el direccionamiento de un servidor TFTP, pide el CTL y los archivos ITL primero.

Esta captura de paquetes muestra una petición del teléfono el archivo ITL. Si usted filtra en el **== 1 tftp.opcode, usted** ve cada TFTP leer la petición del teléfono:

Puesto que el teléfono recibió los archivos CTL e ITL del TFTP con éxito, el teléfono pide un archivo de configuración firmado. Los registros de la consola del teléfono que muestran este comportamiento son disponible desde la interfaz Web del teléfono:

Primero el teléfono pide un archivo CTL, que tiene éxito:

```
837: NOT 09:13:17.561856 SECD: tlRequestFile: Request CTLSEP0011215A1AE3.tlv
846: NOT 09:13:17.670439 TFTP: [27]:Requesting CTLSEP0011215A1AE3.tlv from
14.48.44.80
847: NOT 09:13:17.685264 TFTP: [27]:Finished --> rcvd 4762 bytes
```

El teléfono también pide después un archivo ITL:

```
868: NOT 09:13:17.860613 TFTP: [28]:Requesting ITLSEP0011215A1AE3.tlv from
14.48.44.80
869: NOT 09:13:17.875059 TFTP: [28]:Finished --> rcvd 5438 bytes
```

El teléfono verifica la ITL y el archivo de configuración

Después de que se descargue el archivo ITL, debe ser verificado. Hay varios estados que un teléfono puede estar adentro en este momento, tan estos los documentos abarca ellos todos.

- El teléfono no tiene presente de ningún archivo CTL o ITL o la ITL es en blanco debido al **cluster de la preparación para la restauración no actualizada al** parámetro **pre 8.0**. en este estado, el teléfono confía en ciego el archivo siguiente CTL o ITL descargado y utiliza esta firma en adelante.
- El teléfono tiene ya un CTL pero ninguna ITL. En este estado, el teléfono confía en solamente una ITL si puede ser verificado por la función CCM+TFTP en el archivo CTL.
- El teléfono tiene ya un CTL y un archivo ITL. En este estado, el teléfono verifica que los archivos descargados hagan juego recientemente la firma en el servidor CTL, ITL, o TV.

Aquí está un organigrama que describe cómo el teléfono verifica los archivos firmados y los Certificados HTTPS:

En este caso, el teléfono puede verificar la firma en los archivos ITL y CTL. El teléfono tiene ya un CTL e ITL así que marcó simplemente contra ellos y encontró la firma correcta.

```
877: NOT 09:13:17.925249 SECD: validate_file_envelope:
File sign verify SUCCESS; header length <296>
```

Puesto que el teléfono descargó los archivos CTL e ITL, desde aquí pide SOLAMENTE los archivos de configuración firmados. Esto ilustra que la lógica del teléfono es determinar que el

servidor TFTP es seguro, sobre la base de la presencia de CTL y de ITL, y entonces pedir un archivo firmado:

```
917: NOT 09:13:18.433411 tftpClient: tftp request rcv'd from /usr/tmp/tftp,
srcFile = SEP0011215A1AE3.cnf.xml, dstFile = /usr/ram/SEP0011215A1AE3.cnf.xml
max size = 550001
918: NOT 09:13:18.457949 tftpClient: auth server - tftpList[0] = ::ffff:
14.48.44.80
919: NOT 09:13:18.458937 tftpClient: look up server - 0
920: NOT 09:13:18.462479 SECD: lookupCTL: TFTP SRVR secure
921: NOT 09:13:18.466658 tftpClient: secVal = 0x9 922: NOT 09:13:18.467762
tftpClient: ::ffff:14.48.44.80 is a secure server
923: NOT 09:13:18.468614 tftpClient: retval = SRVR_SECURE
924: NOT 09:13:18.469485 tftpClient: Secure file requested
925: NOT 09:13:18.471217 tftpClient: authenticated file approved - add .sgn
-- SEP0011215A1AE3.cnf.xml.sgn
926: NOT 09:13:18.540562 TFTP: [10]:Requesting SEP0011215A1AE3.cnf.xml.sgn
from 14.48.44.80 with size limit of 550001
927: NOT 09:13:18.559326 TFTP: [10]:Finished --> rcvd 7652 bytes
```

Una vez que se descarga el archivo de configuración firmado, el teléfono debe autenticarlo contra la función para CCM+TFTP dentro de la ITL:

```
937: NOT 09:13:18.656906 SECD: verifyFile: verify SUCCESS
</usr/ram/SEP0011215A1AE3.cnf.xml>
```

El teléfono entra en contacto los TV para el certificado desconocido

El archivo ITL proporciona una función TV que contenga el certificado del servicio TV que se ejecuta en el puerto TCP 2445 del servidor CUCM. Los TV se ejecutan en todos los servidores donde activan al servicio de CallManager. El CUCM servicio TFTP utiliza al grupo de CallManager configurado para construir una lista de servidores TV que el teléfono debe entrar en contacto en el archivo de Configuración del teléfono.

Algunos laboratorios utilizan solamente un solo servidor CUCM. En un cluster del multi-nodo CUCM, puede haber hasta tres entradas TV para un teléfono, uno para cada CUCM en el grupo CUCM del teléfono.

Este ejemplo muestra qué sucede cuando el **botón Directories Button** en el teléfono del IP se presiona. Los directorios URL se configuran para el HTTPS, así que el teléfono se presenta con el certificado de la red de Tomcat del servidor de los directorios. Este certificado de la red de Tomcat (tomcat.pem en la administración OS) no se carga en el teléfono, así que el teléfono debe entrar en contacto los TV para autenticar el certificado.

Refiera al diagrama de descripción anterior TV para una descripción de la interacción. Aquí está la perspectiva del registro de la consola del teléfono:

Primero usted encuentra el directorio URL:

```
1184: NOT 15:20:55.219275 JVM: Startup Module Loader|cip.dir.TandunDirectories:
? - Directory url https://14.48.44.80:8443/ccmcip/xmldirectory.jsp
```

Ésta es una Seguridad de la capa SSL/Transport (TLS) asegura HTTP session que requiere la verificación.

```
1205: NOT 15:20:59.404971 SECD: clpSetupSsl: Trying to connect to IPV4, IP:
14.48.44.80, Port : 8443
1206: NOT 15:20:59.406896 SECD: clpSetupSsl: TCP connect() waiting,
```

```
<14.48.44.80> c:8 s:9 port: 8443
1207: NOT 15:20:59.408136 SECD: clpSetupSsl: TCP connected,
<14.48.44.80> c:8 s:9
1208: NOT 15:20:59.409393 SECD: clpSetupSsl: start SSL/TLS handshake,
<14.48.44.80> c:8 s:9
1209: NOT 15:20:59.423386 SECD: srvr_cert_vfy: Server Certificate
Validation needs to be done
```

El teléfono primero verifica que el certificado presentado por el servidor SSL/TLS esté presente en el CTL. Entonces las miradas del teléfono en las funciones en la ITL clasifían para considerar si encuentra una coincidencia. Este mensaje de error dice el “CERT HTTPS no en el CTL,” que significa “que la certificación no se puede encontrar en el CTL o la ITL.”

```
1213: NOT 15:20:59.429176 SECD: findByCertAndRoleInTL: Searching TL from CTL file
1214: NOT 15:20:59.430315 SECD: findByCertAndRoleInTL: Searching TL from ITL file
1215: ERR 15:20:59.431314 SECD: EROR:https_cert_vfy: HTTPS cert not in CTL,
<14.48.44.80>
```

Después de que el contenido directo del archivo CTL e ITL se marque para saber si hay el certificado, la cosa siguiente los controles del teléfono es el caché TV. Esto se hace para reducir en el tráfico de la red si el teléfono ha pedido recientemente el servidor TV el mismo certificado. Si el certificado HTTPS no se encuentra en el caché del teléfono, usted puede hacer una conexión TCP al servidor TV sí mismo.

```
1220: NOT 15:20:59.444517 SECD: processTvsClntReq: TVS Certificate
Authentication request
1221: NOT 15:20:59.445507 SECD: lookupAuthCertTvsCacheEntry: No matching
entry found at cache
1222: NOT 15:20:59.446518 SECD: processTvsClntReq: No server sock exists,
must be created
1223: NOT 15:20:59.451378 SECD: secReq_initClient: clnt sock fd 11 bound
to </tmp/secClnt_secd>
1224: NOT 15:20:59.457643 SECD: getTvsServerInfo: Phone in IPv4 only mode
1225: NOT 15:20:59.458706 SECD: getTvsServerInfo: Retreiving IPv4 address
1230: NOT 15:20:59.472628 SECD: connectToTvsServer: Successfully started
a TLS connection establishment to the TVS server: IP:14.48.44.80, port:2445
(default); Waiting for it to get connected.
```

Recuerde que la conexión a los TV sí mismo es SSL/TLS (HTTP seguro, o HTTPS), así que es también un certificado que necesita ser autenticado contra la ITL del ot CTL. Si va todo correctamente, el certificado de servidor TV se debe encontrar en la función TV del archivo ITL. Vea ITL #3 de registro en el archivo ITL del ejemplo anterior.

```
1244: NOT 15:20:59.529938 SECD: srvr_cert_vfy: Server Certificate Validation
needs to be done
1245: NOT 15:20:59.533412 SECD: findByIssuerAndSerialAndRoleInTL:
Searching TL from CTL file
1246: NOT 15:20:59.534936 SECD: findByIssuerAndSerialAndRoleInTL:
Searching TL from ITL file
1247: NOT 15:20:59.537359 SECD: verifyCertWithHashFromTL: cert hash and
hash in TL MATCH
1248: NOT 15:20:59.538726 SECD: tvs_cert_vfy: TVS cert verified with hash
from TL, <14.48.44.80>
```

¡Éxito! El teléfono ahora tiene una conexión segura al servidor TV. El siguiente paso es pedir el servidor TV “hola, hace confianza I este certificado de servidor de los directorios?”

Este ejemplo muestra la respuesta a esa pregunta - una respuesta de 0 cuál significa el éxito (ningún error).

```
1264: NOT 15:20:59.789738 SECD: sendTvsClientReqToSrvr: Authenticate
Certificate : request sent to TVS server - waiting for response
1273: NOT 15:20:59.825648 SECD: processTvsSrvrResponse: Authentication Response
```

```
received, status : 0
```

Puesto que hay una respuesta acertada de los TV, los resultados para ese certificado se guardan en el caché. Esto significa que, si usted presiona el **botón Directories Button** otra vez en el plazo de los 86,400 segundos próximos, usted no necesita entrar en contacto el servidor TV para verificar el certificado. Usted puede acceder simplemente caché local.

```
1279: NOT 15:20:59.837086 SECD: saveCertToTvsCache: Saving certificate
in TVS cache with default time-to-live value: 86400 seconds
1287: ERR 15:20:59.859993 SECD: Authenticated the HTTPS conn via TVS
```

Finalmente, usted verifica que su conexión al servidor de los directorios tuviera éxito.

```
1302: ERR 15:21:01.959700 JVM: Startup Module Loader|cip.http.ae:?
- listener.httpSucceed:  https://14.48.44.80:8443/ccmcip/
xmldirectoryinput.jsp?name=SEP0011215A1AE3
```

Aquí está un ejemplo de qué sucede en el servidor CUCM adonde los TV se ejecutan. Usted puede recoger los registros TV con la herramienta unificada Cisco del monitoreo en tiempo real (RTMT).

Los registros CUCM TV muestran que usted contacto SSL con el teléfono, el teléfono pide los TV acerca del certificado de Tomcat, después los TV responde para indicar que el certificado está correspondido con en el almacén de certificados TV.

```
15:21:01.954 |   debug 14.48.44.202: tvsSSLHandShake Session ciphers - AES256-SHA
15:21:01.954 |   debug TLS HS Done for ph_conn .
15:21:02.010 |   debug     MsgType               : TVS_MSG_CERT_VERIFICATION_REQ
15:21:02.011 |   debug tvsGetIssuerNameFromX509 - issuerName : CN=CUCM8-
Publisher.bbbburns.lab;OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US and Length: 75

15:21:02.011 |   debug CertificateDBCache::getCertificateInformation -
Certificate compare return =0
15:21:02.011 |   debug CertificateDBCache::getCertificateInformation -
Certificate found and equal
15:21:02.011 |   debug     MsgType               : TVS_MSG_CERT_VERIFICATION_RES
```

El almacén de certificados TV es una lista de todos los Certificados contenidos en la página web del **Administration (Administración) > Certificate Management (Administración de certificados) OS**.

Verifique manualmente que la ITL del teléfono haga juego la ITL CUCM

Un concepto erróneo común visto mientras que el resolver problemas se refiere a la tendencia a borrar el archivo ITL con la esperanza que resolverá un problema de la verificación del archivo. La cancelacíon del archivo ITL se requiere a veces, pero pudo haber una mejor manera.

El archivo ITL necesita solamente ser borrado cuando TODAS estas condiciones se cumplen.

- La firma del archivo ITL en el teléfono no hace juego la firma del archivo ITL en el servidor TFTP CM.
- La firma TV en el archivo ITL no hace juego el certificado presentado por los TV.
- El teléfono muestra la “verificación no podida” cuando él los attemps para descargar el archivo o los archivos de configuración ITL.
- Ningún respaldo existe de la vieja clave privada TFTP.

Aquí es cómo usted marca los primeros dos de estas condiciones.

Primero, usted puede comparar la suma de comprobación del archivo ITL presente en CUCM con

el archivo ITL de la suma de comprobación del teléfono. No hay actualmente manera de mirar el MD5sum del archivo ITL en CUCM de CUCM sí mismo hasta que usted funcione con una versión con el arreglo para este Id. de bug Cisco CSCto60209.

En el interino, ejecute esto con su favorito GUI o los programas CLI:

```
jasburns@jasburns-gentoo /data/trace/jasburns/certs/SBD $ tftp 14.48.44.80
tftp> get ITLSEP0011215A1AE3.tlv
Received 5438 bytes in 0.0 seconds
tftp> quit
jasburns@jasburns-gentoo /data/trace/jasburns/certs/SBD $ md5sum
ITLSEP0011215A1AE3.tlv
b61910bb01d8d3a1c1b36526cc9f2ddc  ITLSEP0011215A1AE3.tlv
```

Esto muestra que el MD5sum del archivo ITL en CUCM es **b61910bb01d8d3a1c1b36526cc9f2ddc**.

Ahora usted puede mirar el teléfono sí mismo para determinar el hash del archivo ITL cargado allí: **Configuración del > Security (Seguridad) de las configuraciones > lista de la confianza**.

Esto muestra que la coincidencia MD5sums. Esto significa que el archivo ITL en el teléfono hace juego el archivo en el CUCM, así que no necesita ser borrado.

Si corresponde con, usted necesita trasladarse encendido a la operación siguiente - determine independientemente de si el certificado TV en la ITL corresponde con el certificado presentado por los TV. Esta operación está un poco más implicada.

Primero, mirada en la captura de paquetes del teléfono que conecta con los TV el servidor en el puerto TCP 2445.

Haga clic con el botón derecho del ratón en cualquier paquete en esta secuencia en Wireshark, el tecleo **decodifica como**, y selecciona el **SSL**. Encuentre el certificado de servidor que parece esto:

Mire el certificado TV contenido dentro del archivo anterior ITL. Usted debe ver una entrada con el número de serie **2E3E1A7BDAA64D84**.

```
admin:show itl
       ITL Record #:3
                 ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       743
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       TVS
5       ISSUERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       2E:3E:1A:7B:DA:A6:4D:84
```

El éxito, el **TVS.pem dentro del** archivo ITL hace juego el certificado TV presentado en la red. Usted no necesita borrar la ITL, y los TV presentan el certificado correcto.

Si la autenticación del archivo todavía falla, marque el resto del organigrama anterior.

Restricciones e interacciones

Certificados regenerados/reconstrucción un cluster/un vencimiento del certificado

El certificado más importante ahora es el certificado CallManager.pem. La clave privada de este certificado se utiliza para firmar todos los archivos de configuración de TFTP, que incluye el archivo ITL.

Si se regenera el archivo CallManager.pem, un nuevo certificado CCM+TFTP se genera con una nueva clave privada. El archivo ITL ahora es firmado además por esta nueva clave CCM+TFTP.

Después de que usted regenere CallManager.pem y recomience los TV y servicio TFTP, esto sucede cuando un teléfono inicia.

1. Las tentativas del teléfono de descargar el nuevo archivo ITL firmado por el nuevo CCM+TFTP del servidor TFTP. El teléfono tiene solamente el viejo archivo ITL en este momento, y las nuevas claves no están en el archivo ITL presente en el teléfono.
2. Puesto que el teléfono no podría encontrar la nueva firma CCM+TFTP en la vieja ITL, intenta entrar en contacto el servicio TV.
   Nota: Esta parte es extremadamente importante. El certificado TV del viejo archivo ITL debe todavía hacer juego. Si los CallManager.pem y TVS.pem se regeneran en la misma hora exacta, los teléfonos no pueden descargar ninguna nueva archivos sin borrar la ITL del teléfono manualmente.
3. Cuando el teléfono entra en contacto los TV, el servidor CUCM que ejecuta los TV tiene el nuevo certificado CallManager.pem en el almacén de certificados OS.
4. El éxito de las devoluciones del servidor TV y el teléfono carga el nuevo archivo ITL en la memoria.
5. El teléfono ahora intenta descargar un archivo de configuración, que ha sido firmado por la nueva clave CallManager.pem.
6. Puesto que se ha cargado la nueva ITL, el archivo de configuración nuevamente firmado es verificado con éxito por la ITL en la memoria.

Puntos claves:

- Nunca regenere los Certificados CallManager.pem y TVS.pem al mismo tiempo.
- Si se regenera TVS.pem o CallManager.pem, los TV y el TFTP se deben recomenzar y llaman por teléfono a la restauración para obtener los nuevos archivos ITL. Las versiones más recientes de CUCM manejan este teléfono reajustado automáticamente y advierten al usuario en el tiempo de la regeneración del certificado.
- Si existe más de un servidor TV (más de un servidor en el grupo de CallManager), los servidores adicionales pueden autenticar el nuevo certificado CallManager.pem.

Mueva los teléfonos entre los clusteres

Cuando usted mueve los teléfonos a partir de un cluster a otro con ITLs en el lugar, la clave privada ITL y TFTP debe ser tenida en cuenta. Cualquier nuevo archivo de configuración presentado al teléfono DEBE hacer juego una firma en el CTL, la ITL, o una firma en el servicio actual TV del teléfono.

Este documento explica cómo aseegurarse el archivo ITL del nuevo cluster y los archivos de

configuración se pueden confiar en por el archivo actual ITL en el teléfono. https://supportforums.cisco.com/docs/DOC-15799.

De reserva y Restore

El certificado y la clave privada CallManager.pem se sostienen vía el sistema de la Recuperación tras desastres (DR). Si reconstruyen a un servidor TFTP, DEBE ser restablecido del respaldo para poder restablecer la clave privada. Sin la clave privada CallManager.pem en el servidor, los teléfonos con ITLs actual que utilizan la vieja clave no confían en los archivos de configuración firmados.

Si un cluster se reconstruye y no se restablece del respaldo, está exactamente como los "teléfonos móviles entre el documento de los clusteres". Esto es porque un cluster con una nueva clave es un clúster diferente por lo que los teléfonos.

Hay un defecto serio asociado a de reserva y al restore. Si un cluster es susceptible al Id. de bug Cisco CSCtn50405, los respaldos DR no contienen el certificado CallManager.pem. Esto causa cualquier servidor restablecido de este respaldo para generar los archivos corruptos ITL hasta que se genere un nuevo CallManager.pem. Si hay no otros servidores TFTP funcionales que no pasaron con la operación de reserva y del restore, ésta pudo significar que todos los archivos ITL necesitan ser borrados de los teléfonos.

Para verificar si su archivo CallManager.pem necesita ser regenerado, ingrese el **comando del** showitl seguido por:

```
run sql select c.subjectname, c.serialnumber, c.ipv4address, t.name from
certificate as c, certificatetrustrolemap as r, typetrustrole as t where  c.pkid =
r.fkcertificate and t.enum = r.tktrustrole
```

En la salida ITL, los errores dominantes a buscar son:

```
This etoken was not used to sign the ITL file.
```

y

```
Verification of the ITL file failed.
Error parsing the ITL file!!
```

Las búsquedas anteriores de la interrogación del Lenguaje de consulta estructurado (SQL) para los Certificados que tienen un papel de la "autenticación y autorización." El certificado CallManager.pem en la consulta de base de datos anterior que tiene el papel de la autenticación y autorización debe TAMBIÉN estar presente en la página web de la administración de certificados de la administración OS. Si el defecto anterior se encuentra, hay una discordancía entre los Certificados CallManager.pem en la interrogación y en la página web OS.

Cambie los nombres del host o los Domain Name

Si usted cambia el nombre de host o el Domain Name de un servidor CUCM, regenera todos los Certificados inmediatamente en ese servidor. La sección de la regeneración del certificado explicó que la regeneración del TVS.pem y de CallManager.pem es una "mala cosa."

Hay algunos escenarios donde un cambio del nombre de host falla, y algunos donde trabaja sin los problemas. Esta sección cubre todos y los conecta de nuevo al qué usted sabe ya sobre los TV y la ITL de esto documento.

Cluster del nodo único con solamente la ITL (tenga cuidado, esto se rompe sin la preparación)

- Con un negocio Edition Server o el despliegue de Publisher-solamente, los CallManager.pem y TVS.pem se regeneran al mismo tiempo cuando usted cambia los nombres de host.
- Si el nombre de host se cambia en un cluster del nodo único sin primero usando el parámetro Enterprise de la restauración no actualizada cubierto aquí, los teléfonos no pueden verificar el nuevo archivo ITL o los archivos de configuración contra su ITL actual clasifían. Además, no pueden conectar con los TV porque el certificado TV también se confía en no más.
- Los teléfonos visualizan un error sobre “la verificación de la lista de la confianza fallada,” ningunos nuevos cambios de configuración toman el efecto, y el servicio seguro URL falla.
- La única solución si la precaución en el paso 2 no es primera tomada es borrar manualmente la ITL de cada teléfono.

Cluster del nodo único con el CTL e ITL (esto puede estar rota temporalmente, pero ser reparada fácilmente)

- Después de que usted se ejecute con la retitulación de los servidores, vuelva a efectuar al cliente CTL. Esto coloca el nuevo certificado CallManager.pem en el archivo CTL que el teléfono descarga.
- Los nuevos archivos de configuración, que incluyen los nuevos archivos ITL, se pueden confiar en basaron en la función CCM+TFTP en el archivo CTL.
- Esto trabaja porque se confía en el archivo actualizado CTL basó en un USB eToken la clave privada que sigue habiendo lo mismo.

Cluster del Multi-nodo con solamente la ITL (éste trabaja generalmente, pero puede estar roto permanentemente si está hecha de forma precipitada)

- Porque un cluster del multi-nodo tiene servidores múltiples TV, cualquier servidor único puede hacer sus Certificados regenerar sin un problema. Cuando el teléfono se presenta con este nuevo, firma desconocida, pide que otros de los servidores TV verifiquen el nuevo certificado de servidor.
- Hay dos problemas principales que pueden hacer esto fallar:
  Si todos los servidores se retitulan y se reinician al mismo tiempo, ningunos de los servidores TV son accesibles con los Certificados sabidos cuando vienen los servidores y los teléfonos salvaguardia.Si un teléfono tiene solamente un servidor único en el grupo de CallManager, los servidores adicionales TV no diferencian ningún. Vea “el escenario del cluster del nodo único” para resolver esto, o agregue otro servidor al grupo de CallManager del teléfono.

Cluster del Multi-nodo con el CTL e ITL (esto no puede estar rota permanentemente)

- Después de que usted se ejecute con retitule, el servicio TV autentique los nuevos Certificados.
- Incluso si todos los servidores TV son inasequibles por alguna razón, el cliente CTL puede todavía ser utilizado para poner al día los teléfonos con los nuevos Certificados CallManager.pem CCM+TFTP.

TFTP centralizado

Cuando un teléfono con una ITL inicia, pide estos archivos: **CTLSEP** *< dirección MAC >.tlv*, **ITLSEP** *< dirección MAC >.tlv*, y **SEP** *< dirección MAC >.cnf.xml.sgn*.

Si el teléfono no puede encontrar estos archivos, pide el **ITLFile.tlv y el** CTLFile.tlv**, que un** servidor TFTP centralizado proporciona a cualquier teléfono que lo pida.

Con el TFTP centralizado, hay un solo cluster TFTP esas puntas a varios otros clusteres sub. Esto se hace a menudo porque los teléfonos en CUCM múltiple agrupan la parte el mismo alcance de DHCP, y por lo tanto debe tener el mismo servidor TFTP de la opción DHCP 150. Toda la punta de los Teléfonos IP al cluster central TFTP, incluso si se registran a otros clusteres. Este servidor TFTP central pregunta a los servidores TFTP remotos siempre que reciba una petición un archivo que no puede encontrar.

Debido a esta operación, el TFTP centralizado trabaja solamente en un entorno homogéneo ITL. Todos los servidores deben funcionar con la versión 8.x o posterior CUCM, o todos los servidores deben funcionar con las versiones antes de la versión 8.x.

Si un ITLFile.tlv se presenta del servidor TFTP centralizado, los teléfonos no confían en ninguna archivos del servidor TFTP remoto porque las firmas no hacen juego. Esto sucede en una mezcla heterogénea. En una mezcla homogénea, el teléfono pide ITLSEP **<MAC>.tlv que** se tire del cluster remoto correcto.

En un entorno heterogéneo con una mezcla de la pre-versión 8.x y de clusteres de la versión 8.x, “prepare el cluster para la restauración no actualizada al pre 8.0" debe ser habilitado en el cluster de la versión 8.x según lo descrito en el Id. de bug Cisco CSCto87262 y “los parámetros url asegurados del teléfono” configurados con el HTTP en vez del HTTPS. Esto inhabilita con eficacia las funciones ITL en el teléfono.

Preguntas Frecuentes

¿Puedo apagar el SBD?

Usted puede apagar solamente el SBD si los SBD y las ITL trabajan actualmente.

El SBD se puede inhabilitar temporalmente en los teléfonos con el cluster de la preparación para la restauración no actualizada al parámetro Enterprise del pre 8.0" y configurando los “parámetros url asegurados del teléfono” con el HTTP en vez del HTTPS. Cuando usted fija el parámetro de la restauración no actualizada, crea un archivo firmado ITL con las entradas en blanco de la función. El archivo “vacío” ITL todavía se firma, así que el cluster debe estar en el estado funcional de la Seguridad a completamente - antes de que este parámetro pueda ser habilitado.

Después de que se habilite este parámetro y el nuevo archivo ITL con las entradas en blanco se descarga y se verifica, los teléfonos validan cualquier archivo de configuración, no importa quién lo han firmado.

No se recomienda para dejar el cluster en este estado, porque ningunas de las tres funciones metioned previamente (los archivos de configuración autenticados, los archivos de configuración cifrados, y HTTPS URL) están disponibles.

¿Puedo borrar fácilmente el archivo ITL de todos los teléfonos una vez que se pierde el CallManager.pem?

No hay actualmente método para borrar todo el ITLs de un teléfono proporcionado remotamente por Cisco. Por eso los procedimientos y las interacciones descritos en este documento son tan importantes tener en cuenta.

Hay actualmente una mejora sin resolver al Id. de bug Cisco CSCto47052 que pida estas funciones, pero todavía no se han implementado.

En el período intermedio, una nueva función se ha agregado vía el Id. de bug Cisco CSCts01319 que pudo permitir que el Centro de Asistencia Técnica de Cisco (TAC) invierta a la ITL previamente de confianza si está todavía disponible en el servidor. Esto trabaja solamente en ciertos casos donde está el cluster en una versión con esta corrección de defectos, y donde la ITL anterior existe en un respaldo salvado en una ubicación especial en el servidor. Vea el defecto para ver si su versión tiene el arreglo. Entre en contacto el TAC de Cisco para ejecutarse con el Procedimiento de recuperación potencial explicado en el defecto.

Si el procedimiento previó no está disponible, los botones Phone Button se deben avanzar manualmente en el teléfono para borrar el archivo ITL. Éste es el equilibrio que se hace entre la Seguridad y la facilidad de la administración. Para que el archivo ITL sea verdaderamente seguro, él no debe sea quitado fácilmente remotamente.

Incluso con el botón Programado presiona con los objetos simples del protocolo de acceso a objetos (JABÓN) XML, la ITL no puede ser quitado remotamente. Esto es porque, en este momento, el acceso TV (y acceso seguro de la autenticación el URL para validar así el empuje entrante del botón del JABÓN XML se opone) es no funcional. Si la autenticación URL no se configura como segura, puede ser que sea posible al script que la clave clava la orden para borrar una ITL, pero este script no es disponible desde Cisco.

Otras prensas dominantes remotas del script de los métodos para sin usar la autenticación URL pudieron ser disponible desde otro vendedor, pero estas aplicaciones no son proporcionadas por Cisco.

Lo más frecuentemente el método usado para borrar la ITL es un correo electrónico transmitido a todos los usuarios del teléfono que los da instrucciones de la secuencia clave. Si el acceso de las configuraciones se fija **restricto** o **discapacitado**, el teléfono necesita ser restauración de la fábrica, pues los usuarios no tienen acceso al menú de Configuración del teléfono.