Guía de desconfianza de Cisco IOS XE y GuestShell CA Trust eMudhra

Contenido

Propósito

Este documento proporciona una guía para Cisco IOS® XE para la desconfianza de emergencia de las autoridades de certificados raíz e intermedias de eMudhra.

Utilice esta guía para auditar y administrar la confianza de CA para los servicios cuya configuración permite las jerarquías afectadas. La aplicabilidad del producto y la remediación necesaria se definen en la sección informativa de Cisco. Verifique el soporte del comando y el impacto del servicio para su versión de Cisco IOS XE antes de cambiar la confianza.

Información de Cisco: cisco-sa-emudhra-info-ScS22A1r

Certificados de CA de eMudhra afectados: Original y con firma cruzada

Inventario verificado el 29 de octubre de 2026. Se ven afectadas ocho claves de CA que emiten eMudhra: seis para TLS y dos para la firma de código. Cada clave aparece en un certificado de CA original emitido por emSign y un certificado de CA firmado por Sectigo. Por lo tanto, el inventario contiene 16 certificados: 12 certificados TLS y 4 certificados de firma de código.

Cada par original/firmado cruzado tiene el mismo asunto y la misma clave pública, pero un emisor, número de serie y huella digital del certificado SHA-256 diferentes. Los dos formularios proporcionan rutas de certificación alternativas y ambos deben incluirse en una auditoría.

A. Emisores e inventario de certificados afectados

Emisor A — Certificados TLS originales: CN=emSign Root TLS CA - G3, O=eMudhra Technologies Limited, C=IN.

Emisor B — Certificados originales de firma de códigos: CN=emSign Root CS CA - G3, O=eMudhra Technologies Limited, C=IN.

Emisor C — Todos los certificados con firma cruzada: CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB (Sectigo).

Sujetos G3B: O=eMudhra BV, C=NL. Asuntos del G3C: O=eMudhra Inc., C=EE. UU. Cada celda variante enumera su referencia de emisor, serie hexadecimal y huella digital SHA-256 (dos líneas). El relleno cero a la izquierda no cambia un valor de serie.

CA emisora afectada (CN)	Certificado original Emisor/serie (hexadecimal)/SHA-256	Certificado firmado por Sectigo Emisor/serie (hexadecimal)/SHA-256
1. EM DV TLS CA - G3B TLS	Emisor A A4AEE678F23362B4C0E460B772F214 42C4ACCD12C4F59597925E1A08A7A901 02608543809308D50EC427E118BA1493	Emisor C A024FDF4BA66C785CE4A020483858B7 45A883F349AEDFD5F3A649B5498FFB12 1712BA8B448F3F2A91DBC5A766FCDDBE
2. EM OV TLS CA - G3B TLS	Emisor A 6CADA367FB1C100088120EA202D568 98B896625C0C230ADEEC3EB2CF6AAD50 01ECF9156A68644E82374CE5833BC25B	Emisor C E94223BDE92F914E5AB9ACABFDAC3710 5F1DED4D590AF74631290CF073B122A 2AAC6A1FA479778A0BD43579BD832699
3. EM EV TLS CA - G3B TLS	Emisor A C7C41EFE92D825F05EAE841A4A82C1 E7568FE6E12331F4FD7DE61DA4C7559D 0F8EB192A218D4741A3BA75184333838	Emisor C D8F8685E4F2BD9D82402A85A1C1EB731 579480AEA166290BD3C643589E795FC0 D0E54E86505D180F1DFF99EFD3199512
4. EM DV TLS CA - G3C TLS	Emisor A 588B2E3C2BB8CDA13E1A1209254321 0164D7CEAE5BB909C272AF151FF44B11 77AE9B47D9424B94F1D9558C30934D19	Emisor C 91F347F1A5B7D39962B95E0EE4E299D1 62B7F9868263F72F6911FC78CEAF72C1 979158B7368BF648683B2AA39B02E72
5. EM	Emisor A	Emisor C

CA emisora afectada (CN)	Certificado original Emisor/serie (hexadecimal)/SHA-256	Certificado firmado por Sectigo Emisor/serie (hexadecimal)/SHA-256
OV TLS CA - G3C TLS	296926C227A3A1526392B19482A504 CB6E15165AC802E9B3F99F16C25D41F 4E81C21EBDE71AE1B012AC00BF9C7C3F	8D5A4811939EF447D77111CDD9849AE9 748B51C0ED192878FA1D2F948FB529A E1842C5086C4B67F7BE5B2039DE9489
6. EM EV TLS CA - G3C TLS	Emisor A 8009928A64107601AF05FA2F19F109 432EC25F0D28DE9006D97BF752F17BBB 2 CD41F669933FCB072D9A1148D0261F3	Emisor C 05F078752DECE7A1BB8595D303167171 FD9D5C2DBBD4995AB69B8D50C439D952 7B00529199C2FD01B2174EB58F07021F
7. EM OV CS CA - G3B Firma de código	Emisor B 7818933F8F85B4619A2B35FBA83D0A 9E39DE2881273ACC225A149C72BA3E0F 51424963669AB633EE1DC7DF5DB067B4	Emisor C 41E32B73AC185D6CE0D7480BACF84E69 A496E23AC0CAB8155FC9B117B97EAE36 8EFCBB9041AEC8804D5A308D2D01C2D8
8. EM OV CS CA - G3C Firma de código	Emisor B 544B7F922C31AE220A4A922916F6E6 4B2460A466F95FD40113BCDCCA2CEB29 B3B093921DE45474DA7DF48874C630B1	Emisor C D6A5EF613B390F32EF9CDF34F772841 84112972B8E59D14560AE7E711965447 4AAD119990CF3722BFC1E3B91615E1FD

B. Vías de certificación para distinguir

Trayecto TLS original

```
emSign ECC Root CA - G3
  +-- emSign Root TLS CA - G3 (issued by emSign ECC Root CA - G3)
```

```
       +-- Original EM DV/OV/EV TLS CA - G3B or G3C
            +-- TLS identity certificate
```

Ruta de firma de código original (raíz CS de confianza directamente)

```
emSign Root CS CA - G3
  +-- Original EM OV CS CA - G3B or G3C
       +-- Code-signing identity certificate
```

Ruta con firmas cruzadas de Sectigo (TLS y firma de código)

```
AAA Certificate Services
  +-- One of the eight cross-signed CAs listed above
       +-- TLS or code-signing identity certificate
```

Una ruta TLS también puede terminar en emSign Root TLS CA - G3 cuando esa CA es de confianza directa. Los diagramas muestran las relaciones relevantes entre emisores; la ruta aceptada depende de los delimitadores de confianza y de la directiva de validación del servicio consumidor.

Las CAs raíz/principales que se muestran en el ejemplo proporcionan contexto de cadena y no se cuentan entre las ocho claves de emisión comprometidas. La decisión de eliminar o desconfiar de un elemento principal o raíz es independiente de la identificación de una clave intermedia comprometida.

Para la identificación, utilice el emisor del certificado y el número de serie junto con la huella digital SHA-256. Un nombre de asunto por sí solo no es suficiente. Una huella digital de certificado identifica una variante de certificado; un hash SPKI SHA-256 identifica la clave pública compartida por sus formularios originales y con firma cruzada. Quitar sólo un intermedio almacenado en caché no impide que un par lo presente a través de una ruta de acceso de confianza restante.

Fuentes y fecha de verificación

El 29 de octubre de 2026 se verificaron los identificadores de certificados con los archivos adjuntos a los incidentes públicos. Cada par original/con firma cruzada contiene la misma clave pública. Utilice la información en directo de Cisco para conocer el estado de aplicabilidad y remediación del producto.

Información de Cisco: cisco-sa-emudhra-info-ScS22A1r

Registro de incidentes de Mozilla: Compromiso de clave intermedia eMudhra (2083449)

Anexo del certificado de la CA original (9664066)

Anexo de certificado de CA con firma cruzada AAA (9664067)

Manzana: huellas digitales y rutas de certificados TLS originales y con firma cruzada

A partir del 31 de octubre de 2026, la CA raíz de emSign: G1 no se ha identificado entre las CA comprometidas enumeradas en esta guía. Su confianza continua está sujeta a las políticas de su organización y a las posteriores actualizaciones de asesoramiento.

Cómo gestiona Cisco IOS XE la confianza de certificados

Los puntos de confianza PKI configurados contienen certificados de identidad/CA y una política de validación. El conjunto de confianza PKI contiene certificados de CA incorporados y descargados para los servicios que lo utilizan. Identificar la fuente de confianza y la política utilizada por cada servicio relevante; al cambiar el grupo de confianza no se reemplazan los puntos de confianza configurados por separado.

1. Auditoría y preparación

Compruebe la versión del software, la hora del dispositivo y los certificados instalados:

<#root>

```
show version show clock show crypto pki trustpoints show running-config | section crypto pki trustpoint
```

Compare el emisor del certificado completo y el número de serie hexadecimal con el inventario, usando el asunto como contexto de soporte. Cuando Cisco IOS XE muestra solo huellas digitales MD5 y SHA1, la huella digital SHA-256 del inventario no se puede comparar directamente en esa salida; se proporciona para la verificación de los archivos de certificado fuera del dispositivo. El relleno inicial 00 de los números de serie puede diferir. Las búsquedas de nombres de proveedores solo identifican a los candidatos. Registre los servicios que dependen de cada punto de confianza y compruebe las rutas de acceso originales y con firma cruzada, incluidos los

intermediarios de confianza directa.

Examples: CA raíz y SubCA afectada

Se muestran ejemplos abreviados del certificado detallado; se omiten otros campos. Compare el asunto, el emisor y el número de serie.

Ejemplo de CA raíz: EMSign ECC raíz CA - G3

```
CA Certificate
  Certificate Serial Number (hex): 3CF607A968700EDA8B84
  Issuer:
    cn=emSign ECC Root CA - G3
  Subject:
    cn=emSign ECC Root CA - G3
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Ejemplo de subCA afectada: certificado original emitido por emSign

```
CA Certificate
  Certificate Serial Number (hex): 00A4AEE678F23362B4C0E460B772F214
  Issuer:
    cn=emSign Root TLS CA - G3
  Subject:
    cn=EM DV TLS CA - G3B
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Ejemplo de subCA afectada: Certificado firmado por Sectigo

```
CA Certificate
  Certificate Serial Number (hex): 00A024FDF4BA665C785CE4A020483858B7
  Issuer:
    cn=AAA Certificate Services
  Subject:
    cn=EM DV TLS CA - G3B
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Ambos formularios de la subautoridad de certificación tienen el mismo asunto pero emisores y series diferentes. Hacer coincidir el emisor completo y el número de serie con el inventario; el relleno inicial 00 puede diferir. Registre los puntos de confianza asociados para localizar el punto de confianza o conjunto propietario. La raíz que se muestra es el contexto de cadena; no es una de las ocho claves de emisión comprometidas.

Mantenga disponibles un método de acceso de recuperación y un paquete de sustitución aprobado. Utilice el procedimiento aprobado de copia de seguridad de certificados/claves cuando sea necesario. Realice una copia de seguridad de la configuración; esta copia por sí sola no es una copia de seguridad de clave privada:

<#root>

```
copy running-config <BACKUP-CONFIG-URL>
```

Reemplace los marcadores de posición de corchetes angulares por valores específicos de dispositivo aprobados. Utilice un sistema de archivos mostrado por show file systems, como flash: o bootflash:.

2. Revisar rutas de confianza

Quitar subCA afectadas de confianza directa

Elimine las subCA afectadas de confianza directa de los trustpoints y los paquetes de trustpool descargados. No confíe en la configuración de revocación para invalidar la confianza directa en una CA comprometida.

Eliminación de CA raíz opcional

La eliminación de la CA raíz es una recomendación opcional para obtener protección adicional. Una raíz necesaria puede seguir siendo de confianza cuando las comprobaciones de CRL/OCSP de servicio real obtienen el estado actual, evalúan la SubCA afectada bajo un elemento principal de confianza, rechazan las cadenas más largas afectadas originales, con firma cruzada y aplicables, y no superan la validación si ninguno de los métodos configurados proporciona el estado utilizable. En estas condiciones verificadas, la comprobación de revocación protege frente a los emisores comprometidos identificados sin eliminar la raíz.

Considere la posibilidad de eliminar los anclajes raíz/de confianza innecesarios para reducir la dependencia de los servicios de revocación. Evalúe primero las dependencias del servicio: la eliminación de Servicios de Certificate Server de AAA puede interrumpir cadenas legítimas no relacionadas. Cubra las rutas eMudhra y AAA. La eliminación sólo de una SubCA almacenada en caché no bloquea una copia proporcionada por el mismo nivel a través de un padre de confianza restante.

Quitar un punto de confianza seleccionado

Para un punto de confianza configurado por el administrador que se va a eliminar:

<#root>

```
configure terminal no crypto pki trustpoint <TRUSTPOINT-NAME> end
```

Revise la confirmación antes de aceptar. La eliminación de Trustpoint destruye sus certificados asociados. Si es necesario reemplazar una identidad de dispositivo, obtenga un certificado de reemplazo que coincida con la clave de dispositivo y actualice su enlace de servicio mediante el procedimiento de inscripción de servicio. La instalación de un nuevo certificado de CA por sí sola no reemplaza la identidad del dispositivo.

Para las entradas descargadas del conjunto de confianza, utilice el procedimiento de reemplazo del conjunto. Los anclajes integrados o administrados por funciones requieren la actualización del producto compatible o la guía del TAC de Cisco.

3. Actualice el conjunto de confianza descargado, si es necesario

Siga estos pasos cuando sea necesario sustituir un paquete descargado. Un padre/raíz requerido puede seguir siendo confiable bajo las condiciones de revocación verificadas en el Paso 2.

3.1 Comprobar si un paquete descargado está instalado y se utiliza

<#root>

```
show running-config | section crypto pki certificate pool show crypto pki trustpool verbose show crypto
```

Busque las entradas del paquete en el conjunto de certificados crypto pki y los registros de CA marcados como Trustpool: Descargado. Los nombres de archivo del paquete pueden diferir de ios.p7b o ios_core.p7b. Un archivo almacenado o una URL de actualización configurada por sí sola no demuestra que un servicio haya instalado o utilizado sus certificados. Confirme que el servicio utiliza el grupo de confianza y compare sus registros de CA con el inventario afectado. Si no hay ninguna CA descargada instalada, omita la limpieza y el reemplazo; sigue evaluando otras fuentes de confianza.

3.2 Limpie el conjunto de confianza descargado

Mantenga el acceso de recuperación y un paquete de recuperación aprobado disponibles antes de la limpieza. La descarga posterior puede fallar si la transferencia depende de que se elimine la confianza. Plan para la interrupción de los servicios dependientes.

<#root>

```
configure terminal crypto pki trustpool clean end
```

```
show crypto pki trustpool verbose
```

Confirme que los registros de CA descargados no existen. Cleanup quita todos los certificados de trustpool descargados y sus archivos de agrupamiento administrado; las CA integradas y los puntos de confianza independientes permanecen. No guarde hasta que la sustitución y las comprobaciones de servicio se realicen correctamente.

3.3 Obtener e instalar el paquete de sustitución aprobado

Obtenga un paquete aprobado firmado por Cisco. Seleccione ios.p7b o ios_core.p7b para los servicios requeridos y confirme que excluye los certificados afectados y los anclajes de confianza no deseados identificados anteriormente. Los paquetes heredados comprobados el 31 de octubre de 2026 contienen EMSign Root CA - G1 en ios.p7b, pero ni eMudhra ni AAA Certificate Services CA en ios_core.p7b. Core tiene un conjunto de confianza más pequeño: verifique las dependencias del servicio antes de conmutar y verifique el contenido del paquete que instala. Almacénelo fuera del almacén de conjunto de confianza gestionado mediante transferencia HTTPS o SCP aprobada.

Paquete Cisco Full CA: ios.p7b

Paquete de CA principal de Cisco: ios_core.p7b

<#root>

```
show file systems copy <APPROVED-BUNDLE-SOURCE-URL> <STAGED-BUNDLE-URL> configure terminal crypto pki tr
```

Por ejemplo, la dirección URL preconfigurada puede ser flash:approved-ios.p7b. Si la importación falla, restaure un paquete aprobado antes de guardarlo. Verifique las CA deseadas y las conexiones necesarias. La limpieza no es una lista de denegación de certificados: confirme que

los puntos de confianza restantes, las CA integradas y las rutas alternativas rechazan las cadenas afectadas mediante la revocación forzada o la eliminación de la ruta de confianza.

4. Configurar la validación y la política de actualización

Antes de realizar cambios, registre la directiva de grupo de confianza existente, las directivas de punto de confianza afectadas, los enlaces de mapa de certificados y actualice las direcciones URL para que se puedan restaurar si es necesario.

Para los puntos de confianza configurados relevantes:

<#root>

```
configure terminal crypto pki trustpoint <VALIDATION-TRUSTPOINT> revocation-check crl ocsp exit end
```

Para los servicios que utilizan la directiva de grupo de confianza:

<#root>

```
configure terminal crypto pki trustpool policy chain-validation revocation-check crl ocsp exit end show
```

Verifique que la política de trustpool mostrada continúe la validación a la raíz y enumere crl ocsp. El dispositivo intenta primero CRL e intenta OCSP cuando la recuperación de CRL no está disponible. Un resultado revocado no supera la validación cuando se evalúa el certificado afectado. No agregue ninguno cuando se requiera una comprobación de revocación correcta.

Verifique la hora correcta, los puntos finales de estado de CA publicados accesibles, los formatos de respuesta aceptados y la ausencia de excepciones de omisión de revocación aplicables. El estado de las subCA afectadas debe evaluarse bajo un padre de confianza. La confianza directa en esa subentidad emisora de certificados puede detener la validación antes de que se compruebe su elemento primario. Verifique que el servicio real obtenga el estado utilizable y actual y rechace las cadenas afectadas. Si el acceso al servidor de estado y el comportamiento de rechazo no se pueden verificar, no trate la configuración por sí sola como protección confirmada; elimine las rutas de confianza pertinentes cuando lo requiera su plan de mitigación. No agregue ninguno para omitir el estado no disponible.

Actualizar las CRL almacenadas en caché antes de verificar la protección

Una CRL utilizable que ya se encuentra en la base de datos o caché local se puede reutilizar incluso después de que la CA publique una CRL más reciente. Verifique la disponibilidad del servidor de estado y, a continuación, borre las CRLs antiguas antes de validar la protección:

<#root>

```
show crypto pki crls clear crypto pki crl show crypto pki crls
```

El comando clear quita las CRL locales para todos los puntos de confianza; no descarga por sí mismo sustituciones. Confirme que las entradas antiguas han desaparecido y, a continuación, inicie una conexión nueva o una validación de certificado en el servicio afectado. Ejecute show crypto pki crls nuevamente y verifique cada emisor relevante, LastUpdate, NextUpdate y punto de distribución contra la publicación actual de las CA. Incluya la CRL de emisores principales que cubre la SubCA afectada, no solo la CRL de emisores de certificados de identificación. Confirme que se rechazan las cadenas afectadas. El borrado puede afectar temporalmente a las nuevas conexiones mientras se obtienen los datos de estado; conservar validación de cierre a fallos.

Revisar el origen de actualización del paquete

Para los dispositivos conectados, configure de forma opcional el origen de actualización del paquete controlado por vencimiento aprobado:

<#root>

```
configure terminal crypto pki trustpool policy cabundle url <APPROVED-REFRESH-BUNDLE-URL> exit end show
```

Revise todos los orígenes de paquetes configurados. La actualización por expiración no sustituye a una actualización de seguridad inmediata y no debe restaurar una ruta de confianza no deseada.

Filtro de mapa de certificado opcional: cobertura y limitación

Un mapa de certificado de Cisco IOS XE (cert-map) coincide con los atributos del certificado, como el nombre del emisor. Como medida adicional, el filtro puede ayudar a rechazar los certificados de ID (hoja) emitidos directamente por las ocho CA enumeradas. Revise la directiva de certificados de coincidencia existente de los puntos de confianza antes de aplicarla.

El comportamiento fue probado el 29 de octubre de 2026 utilizando identidades de laboratorio en EM DV TLS CA - G3B en dispositivos de laboratorio experimentales. En la validación de certificados de peer PKI, el filtro rechazó una identidad emitida directamente pero no bloqueó una identidad emitida a través de una SubCA secundaria adicional; un emisor legítimo no incluido en la lista pasado. La cobertura de comportamiento utilizó un emisor afectado, con la revocación deshabilitada solo en los puntos de confianza de laboratorio temporales para aislar el filtro. Los saludos de la aplicación y otras versiones no se validaron con este filtro; pruebe el servicio real antes de confiar en él.

<#root>

configure terminal crypto pki certificate map EMSIGN-ISSUER-FILTER 10 issuer-name nc cn=EM DV TLS CA - G

Aquí, nc significa "no contiene". Mantenga las ocho condiciones negativas de nombre de emisor en la misma entrada, secuencia 10: todos deben coincidir para que el certificado pase este filtro. Un emisor directo que coincida con cualquier nombre de la lista no pasa el filtro.

Cisco IOS XE puede mostrar entradas normalizadas; por ejemplo, nombre de emisor nc cn = em dv tls ca - g3b. Este formato en minúsculas y espaciado estaba presente en la prueba de comportamiento. Confirme la asignación y su enlace al punto de confianza de validación que utiliza realmente el servicio:

<#root>

show running-config | section crypto pki certificate map show running-config | section crypto pki trustp

El filtro no proporciona una lista de denegación de CA en toda la cadena. Por ejemplo:

```
Trusted root CA
  +-- Affected SubCA
       +-- New child SubCA
            +-- ID (leaf) certificate
```

El emisor de certificados de ID es la nueva SubCA secundaria, por lo que su filtro de nombre de emisor no identifica la CA afectada más alta en la cadena. Otras comprobaciones, incluidas las restricciones de CA y la revocación, siguen aplicándose. Utilice este filtro solo como protección adicional junto con los procedimientos de validación de revocación y eliminación de raíz opcionales de esta guía. Pruebe los certificados secundarios-SubCA y legítimos emitidos directamente con el servicio real.

Reversión del paso 4

Restaure los métodos de revocación registrados, la configuración de validación de cadena y los enlaces de mapa de certificados. Quite las URL de actualización agregadas por este procedimiento y restaure las URL anteriores que se hayan modificado. Este ejemplo quita sólo la dirección URL de actualización y el enlace de filtro agregados; no restaura las otras configuraciones de políticas:

<#root>

```
configure terminal crypto pki trustpool policy no cabundle url <ADDED-REFRESH-BUNDLE-URL> exit
```

```
crypto pki trustpoint <VALIDATION-TRUSTPOINT> no match certificate EMSIGN-ISSUER-FILTER exit end
```

Ejecute estas eliminaciones sólo donde la dirección URL y el enlace se agregaron mediante este procedimiento. Si se reemplazó un enlace de mapa de certificados anterior, restáurelo. Quite un mapa recién creado sólo después de confirmar que ninguna otra configuración hace referencia a él.

No utilice ninguna política crypto pki trustpool solamente cuando el resultado esperado y aprobado sea el restablecimiento a los valores predeterminados. Este restablecimiento general borra las URL de actualización configuradas y restablece la comprobación de revocación a ninguna; no restaura la política personalizada anterior. La reversión de directivas no restaura los certificados eliminados, revierte el paquete instalado o restaura las CRL borradas. Vuelva a comprobar los servicios necesarios y el rechazo de la cadena afectada antes de guardar.

5. Verificar la protección y guardar

- Confirme que se rechazan las cadenas originales y con firma cruzada afectadas, incluido un intermediario proporcionado por pares. Cuando las cadenas más largas sean relevantes, verifique el rechazo cuando la CA afectada sea más alta en la cadena.
- Confirme que las conexiones legítimas necesarias aún funcionan y que cualquier identidad de reemplazo está vinculada al servicio deseado.
- Comprobar el comportamiento cuando los datos de revocación no estén disponibles. Las sesiones TLS/IPsec existentes no se vuelven a validar automáticamente mediante un cambio de directiva; utilice el procedimiento de reconexión compatible con el servicio cuando sea necesario.

Después de que las comprobaciones tengan éxito:

<#root>

show crypto pki certificates verbose show crypto pki trustpool policy write memory

Verifique la persistencia después de la próxima recarga planificada y, si corresponde, en el dispositivo en espera. Si los resultados difieren de la política de confianza esperada, conserve los registros y póngase en contacto con el TAC de Cisco antes de considerar los cambios de confianza verificados.

Lectura adicional

Gestión de Trustpool PKI de Cisco IOS XE

Cisco: Configuración de certificados firmados de CA con Cisco IOS XE PKI

Cisco: Caché de CRL y comprobación de revocación

Guía de confianza de CA GuestShell de Cisco IOS XE

Paso 1: Auditar el estado de implementación de GuestShell del dispositivo

La remediación sólo es necesaria en sistemas Cisco IOS XE en los que GuestShell está instalado y en el estado EN EJECUCIÓN o IMPLEMENTADO. Si GuestShell se encuentra en el estado DEPLOYED, primero debe habilitarse con el comando 'guestShell enable' antes de ejecutar los comandos de corrección. Si show app-hosting list indica 'No App found' (GuestShell no está implementado o habilitado), no se requiere ninguna acción en GuestShell.

A. GuestShell en estado DESPLEGADO (Acción requerida: Debe activar primero)

Cuando show app-hosting list informa que GuestShell está en el estado DEPLOYED, existe almacenamiento en contenedor de GuestShell pero se detiene el contenedor. Debe ejecutar 'guestshell enable' antes de ingresar bash (y opcionalmente 'guestshell disable' después de completar la remediación si regresa a un estado detenido):

<#root>

```
Router#

show app-hosting list

App id                                   State
---------------------------------------------------------
guestshell                               DEPLOYED
```

B. GuestShell en estado RUNNING (acción requerida: Proceda directamente)

Cuando show app-hosting list informa a GuestShell en el estado RUNNING, GuestShell se está ejecutando activamente y puede continuar directamente en bash:

<#root>

```
Router#

show app-hosting list

App id                                   State
---------------------------------------------------------
guestshell                               RUNNING
```

B. GuestShell no habilitado/no implementado (no se requiere ninguna acción)

Si show app-hosting list indica No App found, GuestShell no está instalado o habilitado en el sistema y no se requiere ninguna otra acción:

<#root>

```
Router#

show app-hosting list

No App found
```

Paso 2: Acceso a GuestShell y aplicación de la desconfianza de CA

Ejecute estos comandos desde el mensaje EXEC privilegiado ('enable') de Cisco IOS XE. Si GuestShell está en estado DEPLOYED, habilítelo primero. A continuación, ingrese el shell bash, escale a root y configure la lista de bloqueo de CA usando la selección de carpeta dinámica para

garantizar la compatibilidad entre todas las versiones de Cisco IOS XE:

<#root>

```
! 1. If GuestShell is in DEPLOYED state, enable it first:
Router#
```

guestshell enable

```
! 2. Enter GuestShell bash shell:
Router#
```

guestshell run bash

```
! 3. Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$
```

sudo -s

```
! 4. Prepare the ca-trust blocklist directory (compatible with 17.15.x and 17.18.x):
d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist
mkdir -p "$d"
```

Desconfiando de certificados eMudhra comprometidos

Ejecute los comandos de extracción de confianza para extraer cada certificado de eMudhra comprometido directamente en el directorio de lista de bloqueo de ca-trust, seguido de reconstruir el almacén de confianza del sistema:

```
trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20G3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_G3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=Comodo%20AAA%20Services%20root;type=cert' \
  "$d/Comodo_AAA_Services_root.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20C3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_C3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;type=cert' \
  "$d/emSign_Root_CA_-_C1.pem"

update-ca-trust extract
```

Paso 3: Verificación de certificados desconfiados en GuestShell

Compruebe que los cuatro certificados extraídos aparecen en la directiva de desconfianza/lista de bloqueo del sistema y que están excluidos de los anclajes de confianza activos mediante el comando de verificación siguiente. El comando confirma que los certificados están registrados en la directiva de lista de bloqueo.

```
###Verify with below command
[guestshell@guestshell ~]$ trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign
    label: AAA Certificate Services
    trust: distrusted
    category: authority

--
    label: emSign ECC Root CA - C3
    trust: distrusted
    category: authority

--
    label: emSign ECC Root CA - G3
    trust: distrusted
    category: authority

--
    label: emSign Root CA - C1
    trust: distrusted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
    category: authority

Output will vary based on CentOS Stream version
###Verify CentOS Stream Version
[guestshell@guestshell ~]$ cat /etc/redhat-release
CentOS Stream release 8

OS                          CentOS Stream 8       CentOS Stream 9
Directory                   blacklist only        blocklist
Result shown                 trust: blacklisted    trust: distrusted
```

Paso 4: Persistencia de estado y ciclo de vida del contenedor

Nota sobre la persistencia del contenedor: Estas modificaciones de desconfianza de certificados persisten entre las operaciones 'guestshell enable' e 'guestshell disable' y los reinicios de dispositivos porque /etc/pki/ca-trust reside en el almacenamiento de contenedor persistente.

Volver al estado DESPLEGADO (si procede): Si GuestShell estaba originalmente en el estado

DEPLOYED y habilitado únicamente para ejecutar este procedimiento de desconfianza, devuelva GuestShell a su estado detenido anterior saliendo de bash y ejecutando 'guestShell disable' desde el mensaje EXEC privilegiado del IOS:

<#root>

```
[root@guestshell ~]#

exit

[guestshell@guestshell ~]$

exit

Router#

guestshell disable
```

Consideración importante del ciclo de vida: Si GuestShell se destruye completamente con 'guestshell destroy', se elimina el sistema de archivos contenedor. Si posteriormente se vuelve a habilitar GuestShell, el contenedor se vuelve a crear a partir de la imagen de sistema base y se deben volver a aplicar estos pasos de solución de desconfianza.

Paso 5: Procedimiento de reversión (restauración de la confianza de la CA)

Para invertir la configuración de desconfianza y restaurar la confianza predeterminada de CA en cualquier versión de Cisco IOS XE, seleccione dinámicamente el directorio de lista de bloqueo activo ($d), quite específicamente los cuatro archivos de certificado agregados por este procedimiento (incluida la raíz de Comodo AAA Services) y vuelva a generar el almacén de confianza:

<#root>

```
! Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$

sudo -s



d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

! Remove only the four certificate files added during remediation:
rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \
      "$d/emSign_ECC_Root_CA_-_C3.pem" "$d/emSign_Root_CA_-_C1.pem"
```

```
! Rebuild the system CA trust store:
update-ca-trust extract
```

Verifique que el directorio blocklist ya no contenga los archivos eliminados:

<#root>

```
[root@guestshell ~]#

ls -l "$d"/

total 0
```

Confirmar restauración de confianza de CA: Verifique que los cinco certificados hayan regresado a los anclajes de confianza activos volviendo a ejecutar el comando de verificación del paso 3 (todas las entradas informan confianza: ancla):

<#root>

```
[root@guestshell ~]#

trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
```

Ejemplo de Transcripción de Ejecución de Extremo a Extremo

La transcripción ilustra una auditoría, remediación y sesión de verificación completa y exitosa de GuestShell en un dispositivo Cisco IOS XE:

<#root>

```
Router#

guestshell run bash

[guestshell@guestshell ~]$ sudo -s
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist
```

```
bash-4.4#
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist
bash-4.4#
mkdir -p "$d"
bash-4.4#
trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-
bash-4.4#
trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=Comodo%20AAA%20Services%20ro
bash-4.4#
trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-
bash-4.4#
trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;
bash-4.4#
update-ca-trust extract
bash-4.4#
trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

    label: emSign ECC Root CA - G3
    trust: blacklisted
    category: authority

--
    label: AAA Certificate Services
    trust: blacklisted
    category: authority

--
    label: emSign ECC Root CA - C3
    trust: blacklisted
    category: authority

--
    label: emSign Root CA - C1
    trust: blacklisted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
```

```
    category: authority

bash-4.4#

cat /etc/redhat-release

CentOS Stream release 8
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \ >       "$d/emSign_ECC_Root_C

bash-4.4#
bash-4.4#

update-ca-trust extract

bash-4.4#

ls -l "$d"/

total 0
```

Matriz de resumen de comandos

Tarea operativa	
Auditar estado de GuestShell	`show app-hosting list`
Habilitar GuestShell (si está IMPLEMENTADO)	`guestshell enable`
Ingrese	`guestshell run bash`

GuestShell Bash	
Cambiar a usuario raíz	`sudo -s`
Preparar directorio de lista de bloqueo	`d=/etc/pki/ca-trust/source/blocklist; [ -d "$d" ] || d=/etc/pki/ca-trust/source/blac`
Extraer entidades emisoras de certificados a lista de bloqueo	`trust extract --overwrite --format=pem-bundle ... (x4 CAs)`
Reconstruir el almacén de confianza de CA	`update-ca-trust extract`
Verificar política de desconfianza	`trust list --filter=trust-policy --purpose=server-auth`
Restaurar el estado IMPLEMENTADO (opcional)	`guestshell disable`
Revertir/restaurar confianza	`rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" "$d/emSign_`

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).