

Guía de IOS XR - Desconfianza de emergencia de las autoridades de certificados raíz eMudhra e intermedias

Contenido

Introducción

Descubra cómo identificar y mitigar la exposición de certificados de eMudhra en routers Cisco IOS XR, incluidas las comprobaciones de certificados y los pasos de remediación.

Antecedentes

Este documento proporciona orientación operativa y procedimientos de mitigación interinos para las plataformas de ruteo de Cisco Service Provider que ejecutan Cisco IOS XR, que incluyen:

- Cisco ASR serie 9000
- Cisco Serie 8000
- Cisco NCS serie 1000
- Cisco NCS serie 4000
- Cisco NCS serie 5500
- Cisco NCS serie 6000
- Cisco NCS serie 540/560
- Cisco XRv 9000

Estos procedimientos abordan la exposición potencial asociada con las autoridades de certificados de eMudhra comprometidas, como se documenta en [Cisco Security Advisory cisco-sa-emudhra-info-ScS22A1r](https://www.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r).

El artículo explica cómo identificar los certificados relevantes en el almacén de certificados de IOS XR Linux, evaluar la exposición potencial y aplicar procedimientos de mitigación provisionales cuando corresponda.

Vulnerabilidad y contexto de amenazas

Entre el 17 y el 20 de octubre de 2026, se hizo público un defecto criptográfico sin precedentes en la Ceremonia de Generación de Claves (KGC) de abril de 2025 en eMudhra. Debido a la falta de aleatoriedad durante la generación de claves, las claves privadas de ocho (8) autoridades de certificados intermedios de eMudhra (6 CA emisoras de TLS y 2 CA de firma de código) se pueden factorizar y derivar en segundos por agentes no autorizados.

Factor de composición crítico (firma cruzada de Sectigo): En mayo de 2025, las ocho CA intermedias comprometidas fueron firmadas por Sectigo legacy root (AAA Certificate Services). Debido a que la raíz de Sectigo está integrada de forma ubicua en almacenes de confianza públicos y empresariales, los certificados emitidos por estas CA intermedias comprometidas son de confianza de forma predeterminada en todos los sistemas operativos y pilas TLS globalmente, incluso si la raíz nativa de eMudhra está ausente.

Arquitectura de certificados y análisis de exposición de Cisco IOS XR

Las aplicaciones IOS XR utilizan de forma predeterminada el almacén de certificados XR. Hay dos certificados eMudhra incluidos en el paquete de CA de Linux IOS XR. Sólo se utilizan en tres escenarios específicos, cuando:

- La línea de comandos de Linux se utiliza para ejecutar curl o wget contra un servidor HTTPS
- Se accede a LDAP a través de TLS
- Opflex está implementado (solo en la serie ASR 9000)

Auditoría e identificación de certificados y puntos de confianza configurados

Cualquier versión de Cisco IOS XR anterior a la 26.4.1 (que se lanzará el 30 de noviembre de 2026) contiene estos certificados de CA. Para validar que estos certificados están presentes en un dispositivo XR, acceda a XR Linux CLI y verifique el contenido del archivo certificates.conf:

```
<#root>
```

```
RP/0/RP0/CPU0:Router#
```

```
run
```

```
[xr-vm_node0_RP0_CPU0:~]$
```

```
grep "Comodo_AAA_Services_root.crt\|emSign_ECC_Root_CA_-_G3.crt" /etc/ca-certificates.conf
```

```
mozilla/Comodo_AAA_Services_root.crt
```

```
mozilla/emSign_ECC_Root_CA_-_G3.crt
```

Si se mencionan uno o ambos certificados en los certificados, busque la ruta de acceso de ambos archivos:

```
<#root>
```

```
[xr-vm_node0_RP0_CPU0:~]$
```

```
find / -type f \( -name "Comodo_AAA_Services_root.crt" -o -name "emSign_ECC_Root_CA_-_G3.crt" \) 2>/dev/null
```

```
/usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt  
/usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
```

Si estos archivos están presentes y se hace referencia a ellos en certificates.conf, su dispositivo podría ser explotado.

Procedimientos de remediación

Los pasos de mitigación son:

- agregue un ! al principio de cada archivo certificate.conf
- quitar certificados encontrados
- actualizar el archivo certificate.conf

Para versiones de eXR:

Agregue un ! al principio de cada archivo certificate.conf

```
<#root>
```

```
[xr-vm_node0_RP0_CPU0:~]$
```

```
cat /etc/ca-certificates.conf | grep "Comodo_AAA_Services_root.crt|emSign_ECC_Root_CA_-_G3.crt"
```

```
!mozilla/Comodo_AAA_Services_root.crt  
!mozilla/emSign_ECC_Root_CA_-_G3.crt
```

Quitar certificados encontrados

```
<#root>
```

```
[xr-vm_node0_RP0_CPU0:~]$
```

```
rm /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt
```

```
[xr-vm_node0_RP0_CPU0:~]$
```

```
rm /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
```

Actualizar archivo certificate.conf

```
<#root>
```

```
[xr-vm_node0_RP0_CPU0:~]$update-ca-certificates
```

```
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt, it does not contain exactly one certificate or CRL
0 added,
2 removed;
done.
```

Aunque este procedimiento termina siendo simple, debe repetirse en cada VM (default-sdr y sysadmin para cada nodo) y en el sistema operativo host del router.

Este procedimiento se puede automatizar ejecutando una secuencia de comandos de shell:

- Cargue y copie el script en la máquina virtual de administración en el RP activo

<#root>

sysadmin-vm:0_RP0#

copy harddisk:exr_remove_eMudhra_cert.sh harddisk: location 0/RP0/CPU0/VM1

Tue Oct 27 01:59:29.149 UTC+00:00

Copying harddisk:exr_remove_eMudhra_cert.sh to harddisk:

exr_remove_eMudhra_cert.sh 100% 1604 4.3MB/s 00:00

File copied successfully

- Ir a la VM de administración del RP activo

<#root>

RP/0/RP0/CPU0:Router#

admin

Last login: Mon Oct 26 22:46:01 2026 from 192.0.2.4

user connected from 192.0.2.4 using ssh on sysadmin-vm:0_RP0

sysadmin-vm:0_RP0#

run

[sysadmin-vm:0_RP0:~]\$

- Ejecutar el script

<#root>

```
[sysadmin-vm:0_RP0:~]$.
```

```
/exr_remove_eMudhra_cert.sh
```

```
== Local sysadmin VM (sysadmin-vm:0_RP0) ==
```

```
-- /etc/ca-certificates.conf entries:
```

```
!mozilla/Comodo_AAA_Services_root.crt
```

```
!mozilla/emSign_ECC_Root_CA_-_G3.crt
```

```
found: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt
```

```
deleted: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt
```

```
found: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
```

```
deleted: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
```

```
--
```

```
Validation (expect: ls: cannot access '/etc/ssl/certs/...pem': No such file or directory):
```

```
ls: cannot access '/etc/ssl/certs/Comodo_AAA_Services_root.pem': No such file or directory
```

```
ls: cannot access '/etc/ssl/certs/emSign_ECC_Root_CA_-_G3.pem': No such file or directory
```

```
== Local host (my_host) ==
```

```
-- /etc/ca-certificates.conf entries:
```

```
!mozilla/Comodo_AAA_Services_root.crt
```

```
!mozilla/emSign_ECC_Root_CA_-_G3.crt
```

```
found: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt
```

```
deleted: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt
```

```
found: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
```

```
deleted: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
```

```
-- Validation (expect: ls: cannot access '/etc/ssl/certs/...pem': No such file or directory):
```

```
ls: cannot access '/etc/ssl/certs/Comodo_AAA_Services_root.pem': No such file or directory
```

```
ls: cannot access '/etc/ssl/certs/emSign_ECC_Root_CA_-_G3.pem': No such file or directory
```

```
== lc0_xr ==
```

```
-- /etc/ca-certificates.conf entries:
```

```
!mozilla/Comodo_AAA_Services_root.crt
```

```
!mozilla/emSign_ECC_Root_CA_-_G3.crt
```

```
found: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
```

```
deleted: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
```

```
found: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt
```

```
deleted: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt
```

```
-- Validation (expect: ls: cannot access '/etc/ssl/certs/...pem': No such file or directory):
```

```
ls: cannot access '/etc/ssl/certs/Comodo_AAA_Services_root.pem': No such file or directory
```

```
ls: cannot access '/etc/ssl/certs/emSign_ECC_Root_CA_-_G3.pem': No such file or directory
```

```
== rp0_xr ==
```

```
-- /etc/ca-certificates.conf entries:  
!mozilla/Comodo_AAA_Services_root.crt  
!mozilla/emSign_ECC_Root_CA_-_G3.crt  
found: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt  
deleted: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt  
found: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt  
deleted: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt  
-- Validation (expect: ls: cannot access '/etc/ssl/certs/...pem': No such file or directory):  
ls: cannot access '/etc/ssl/certs/Comodo_AAA_Services_root.pem': No such file or directory  
ls: cannot access '/etc/ssl/certs/emSign_ECC_Root_CA_-_G3.pem': No such file or directory  
Done.
```

En todas las VM y el sistema operativo host, los nombres de los certificados se comentarán en certificates.conf; los certificados se eliminarán y actualizarán.

Enlace de script: <https://cisco.box.com/s/mevtcydjarl2tz0rc39862x100b8x3mu>

Para las versiones XR7:

El procedimiento para las versiones XR7 aún está en revisión.

Referencias

1. [Asesoría en seguridad de Cisco: cisco-sa-emudhra-info-ScS22A1r](#)
2. [Blog de Cisco Talos: Certificados intermedios eMudhra comprometidos](#)

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).