

IOS XR Guidance - Noodsituatie wantrouwen van Mudhra Root en Intermediate Certificate Autoriteiten

Inhoud

Inleiding

Leer hoe u eMudhra-certificaatblootstelling op Cisco IOS XR-routers kunt identificeren en beperken, inclusief certificaatcontroles en herstelstappen.

Achtergrondinformatie

Dit document biedt operationele richtlijnen en tussentijdse procedures voor het beperken van risico's voor Cisco Service Provider-routeringsplatforms met Cisco IOS XR, waaronder:

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

Deze procedures hebben betrekking op mogelijke blootstelling in verband met de gecompromitteerde eMudhra Certificate Authorities, zoals gedocumenteerd in [Cisco Security Advisory cisco-sa-emudhra-info-ScS22A1r](#).

In het artikel wordt uitgelegd hoe relevante certificaten in de IOS XR Linux-certificaatopslag kunnen worden geïdentificeerd, mogelijke blootstelling kan worden beoordeeld en waar van toepassing tussentijdse mitigatieprocedures kunnen worden toegepast.

Kwetsbaarheid en dreigingscontext

Tussen 17 oktober en 20 oktober 2026 werd een ongekend cryptografisch defect in de Key Generation Ceremony (KGC) van april 2025 in Meudhra openbaar gemaakt. Als gevolg van verbroken willekeur tijdens het genereren van sleutels kunnen de privésleutels voor acht (8) intermediaire certificeringsautoriteiten van Mudhra (6 TLS-certificeringsautoriteiten en 2-codeondertekeningsbevoegde autoriteiten) binnen enkele seconden door niet-geautoriseerde actoren worden gefactoriseerd en afgeleid.

Critical Compounding Factor (Sectigo Cross-Signature): In mei 2025 werden alle acht gecompromitteerde intermediaire CA's ondertekend door Sectigo legacy root (AAA Certificate Services). Omdat root van Sectigo alomtegenwoordig is ingebed in openbare en zakelijke vertrouwenswinkels, worden certificaten die zijn uitgegeven door deze gecompromitteerde intermediaire CA's standaard vertrouwd op besturingssystemen en TLS-stacks wereldwijd, zelfs als de native eMudhra-root afwezig is.

Cisco IOS XR-certificaatarchitectuur en blootstellingsanalyse

IOS XR-toepassingen gebruiken standaard XR-certificaatarchief. Er zijn twee eMudhra-certificaten opgenomen in de IOS XR Linux CA-bundel. Ze worden alleen gebruikt in drie specifieke scenario's, wanneer:

- De Linux-opdrachtregel wordt gebruikt voor het uitvoeren van curl of wget tegen een HTTPS-server
- LDAP is toegankelijk via TLS
- Opflex wordt geïmplementeerd (alleen op ASR 9000-reeks)

Geconfigureerde Trustpoints en certificaten controleren en identificeren

Elke Cisco IOS XR-versie vóór 26.4.1 (die op 30 november 2026 wordt uitgebracht) bevat deze CA-certificaten. Om te bevestigen dat deze certificaten aanwezig zijn op een XR-apparaat, hebt u toegang tot XR Linux CLI en verifieert u de inhoud van het bestand `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
```

Als een of beide certificaten op de certificaten staan vermeld, zoek dan naar het pad van beide bestanden:

```
<#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
```

Als deze bestanden aanwezig zijn en worden verwezen in certificates.conf, kan uw apparaat worden geëxploiteerd.

saneringsprocedures

Mitigerende stappen bestaan uit:

- Voeg een! toe aan het begin van elk Certificate.conf-bestand
- Gevonden certificaten verwijderen
- Certificate.conf-bestand bijwerken

Voor eXR-releases:

Een! toevoegen aan het begin van elk bestand 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
```

Gevonden certificaten verwijderen

<#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
```

Certificate.conf-bestand bijwerken

<#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.
```

Hoewel deze procedure uiteindelijk eenvoudig is, moet deze worden herhaald op elke VM (standaard-sdr en sysadmin voor elk knooppunt) en het hostbesturingssysteem van de router.

Deze procedure kan worden geautomatiseerd door een shell script uit te voeren:

- Upload en kopieer het script naar de admin-VM op de actieve RP

<#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
```

- Ga naar admin VM van de actieve RP

<#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:~]$
```

- Het script uitvoeren

<#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.
```

Op alle VM's en het hostbesturingssysteem zullen certnamen worden becommentarieerd op certificates.conf, certificaten worden verwijderd en bijgewerkt.

Scriptlink: <https://cisco.box.com/s/mevtcydjarl2tz0rc39862x100b8x3mu>

Voor XR7-releases:

De procedure voor XR7-releases wordt nog onderzocht.

Referenties

1. [Cisco Security Advisory: cisco-sa-emudhra-info-ScS22A1r](#)
2. [Cisco Talos Blog: gecompromitteerde eMudhra-intermediaire certificaten](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.