

IOS XR Guidance - Emergency Distrust of eMudhra Root and Intermediate Certificate Authorities

Contents

Introduction

Learn how to identify and mitigate eMudhra certificate exposure on Cisco IOS XR routers, including certificate checks and remediation steps.

Background Information

This document provides operational guidance and interim mitigation procedures for Cisco Service Provider routing platforms running **Cisco IOS XR**, including:

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

These procedures address potential exposure associated with the compromised **eMudhra Certificate Authorities**, as documented in [Cisco Security Advisory cisco-sa-emudhra-info-ScS22A1r](https://www.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r).

The article explains how to identify relevant certificates in the IOS XR Linux certificate store, assess potential exposure, and apply interim mitigation procedures where applicable.

Vulnerability & Threat Context

Between October 17 and October 20, 2026, an unprecedented cryptographic defect in the April 2025 Key Generation Ceremony (KGC) at eMudhra was publicly disclosed. Due to broken randomness during key generation, the private keys for **eight (8) eMudhra Intermediate Certificate Authorities** (6 TLS Issuing CAs and 2 Code Signing CAs) can be factorized and derived by unauthorized actors within seconds.

Critical Compounding Factor (Sectigo Cross-Signature): In May 2025, all eight compromised intermediate CAs were cross-signed by Sectigo legacy root (AAA Certificate Services). Because root from Sectigo is ubiquitously embedded in public and enterprise trust stores, certificates issued by these compromised intermediate CAs are trusted by default across operating systems and TLS stacks globally, even if the native eMudhra root is absent.

Cisco IOS XR Certificate Architecture & Exposure Analysis

IOS XR applications by default use XR certificate store. There are two eMudhra certificates included in the IOS XR Linux CA bundle. They are only used in three specific scenarios, when:

- The Linux command line is used to run **curl** or **wget** against an HTTPS server
- LDAP is accessed over TLS
- Opflex is implemented (only on ASR 9000 Series)

Audit and Identify Configured Trustpoints & Certificates

Any Cisco IOS XR version prior to 26.4.1 (to be released on Nov 30, 2026) contains these CA certificates. To validate that these certificates are present on a XR device, access to XR Linux CLI and verify the content of the certificates.conf file:

```
<#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
```

If one or both certificates are mentioned on the certificates are present, then look for the path of both files:

```
<#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
```

If these files are present and are referenced in certificates.conf, your device could be exploited.

Remediation Procedures

Mitigation steps consist on:

- add a ! at the beginning of every the certificate.conf file
- remove found certificates
- update certificate.conf file

For eXR Releases:

Add a ! at the beginning of every the certificate.conf file

<#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
```

Remove found certificates

<#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
```

Update certificate.conf file

<#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.
```

Although, this procedure ends up being simple, **but it needs to be repeated on every VM** (default-sdr and sysadmin for every node) **and the host OS** of the router.

This procedure can be automated by running a shell script:

- Upload and copy the script to the admin VM on the active 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

- Go to admin VM of the active 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:~]\$

- Execute the 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.
```

On all VMs and host OS, Cert names are going to get commented on certificates.conf, certificates are going to be removed and updated.

Script link: <https://cisco.box.com/s/mevtcydjarl2tz0rc39862x100b8x3mu>

For XR7 Releases:

Procedure for XR7 releases is still under review.

References

1. [Cisco Security Advisory: cisco-sa-emudhra-info-ScS22A1r](#)
2. [Cisco Talos Blog: Compromised eMudhra Intermediate Certificates](#)