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** software, including:

- Cisco 8000 Series
- Cisco ASR 9000 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.

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 cerficates 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/

```
/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.

Classic IOS XR versions (32-bit) are not affected byt this issue.

Remediation Procedures

Mitigation steps consist on:

- Prepend a “!” to the beginning of every line containing affected certificates on the certificate.conf file
- Remove found certificates
- Update and syncronize system-wide SSL/TLS Certificates

For eXR Releases

Prepend a “!” to the beginning of every line containing affected certificates on the certificate.conf file

<#root>

```
    [xr-vm_node0_RP0_CPU0:~]$

sed -i -E '/Comodo_AAA_Services_root\.crt|emSign_ECC_Root_CA_-_G3\.crt/s/^/!/' /etc/ca-certificates.conf

[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
```

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 and syncronize system-wide SSL/TLS Certificates

<#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. Then access to Linux CLI of the admin VM (for NCS 560 routers, the script must be executed on the XR VM Linux CLI)

<#root>

```
    sysadmin-vm:0_RP0#
```

```
copy harddisk:asr9k_remove_eMudhra_cert.sh location 0/RP0/CPU0/VM1 harddisk:
```

```
Tue Oct 27 01:59:29.149 UTC+00:00
Copying harddisk:asr9k_remove_eMudhra_cert.sh to harddisk:
asr9k_remove_eMudhra_cert.sh 100% 2410 2.4KB/s 00:00
```

```
File copied successfully
```

```
sysadmin-vm:0_RP0#
sysadmin-vm:0_RP0#
```

```
run
```

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

Add execute permission and run the script

<#root>

[sysadmin-vm:0_RP1:~]$

chmod +x asr9k_remove_eMudhra_cert.sh

[sysadmin-vm:0_RP0:~]$

./asr9k_remove_eMudhra_cert.sh

===== local node (this XR VM) =====

-- Entries found in /etc/ca-certificates.conf:

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

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.

Running hooks in /etc/ca-certificates/update.d...

asr9k_remove_eMudhra_cert.sh

===== lc0_admin =====

-- Entries found in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.
```

===== lc0_xr =====

```
-- Entries found in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.
```

===== my_host =====

```
-- Entries found in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.
```

===== rsp0_xr =====

```
-- Entries found in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.
```

===== rsp1_admin =====

```
-- Entries found in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.
```

===== rsp1_xr =====

```
-- Entries found in /etc/ca-certificates.conf:
```

```
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.
```

On all VMs and host OS where Admin VM can access, cert names are going to get commented on certificates.conf, certificates are going to be removed and updated.

Current available scripts are:

- **ASR 9000 Router Series -** https://cisco.app.box.com/file/2557835175620?s=tmogb804gb75pdy2nrivm9jfp84ybqyt
- **NCS 540 and 5500 Router Series -** https://cisco.app.box.com/file/2557840859193?s=1t79efmqk8g3ppnyoegmt5iu6q0xps01
- **NCS 560 Router Series -** https://cisco.app.box.com/s/co7k52pwayjs7nx1toyse0g56a34gnrd

If script execution hangs, one or more hosts are likely prompting for a password. In that case, perform the remediation procedure manually.

For XR7 Releases

Cisco IOS XR7 Software uses SELinux, and enforcement was enabled on different platforms in the following releases:

- Cisco 8000 (x86_64): enforcement enabled in 24.4.1
- NCS 540L: enforcement enabled in 26.1.1
- NCS 5700: enforcement enabled in 26.2.1
- NCS 1000 (Lindt): enforcement enabled in 26.3.1

Verify enforcement status. If Permissive is returned, manual remediation or script can be executed. If Enforcing is returned, upgrade to the 26.4.1 release.

<#root>

```
RP/0/RP0/CPU0:
```

Router-1

#

run

```
[node0_RP0_CPU0:~]$
```

getenforce

Enforcing

```
RP/0/RP0/CPU0:
```

Router-2

```
#
```

run

```
[node0_RP0_CPU0:~]$
```

getenforce

Permissive

Upload the script to the active RP. Then access to Linux CLI and change to the harddisk directory

<#root>

RP/0/RP0/CPU0:Router#

run

```
[node0_RP0_CPU0:~]$
```

cd /misc/disk1

```
[node0_RP0_CPU0:/misc/disk1]$
```

Add execute permission and run the script

<#root>

[node0_RP0_CPU0:/misc/disk1]$

```
chmod +x xr7_remove_eMudhra_cert.sh


[node0_RP0_CPU0:/misc/disk1]$

./xr7_remove_eMudhra_cert.sh


================ LOCAL NODE ================
Node: node0_RP0_CPU0
-- Matching lines in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
[RUN] prepend '!' to matching lines in /etc/ca-certificates.conf
[RUN] rm -f /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt
[RUN] rm -f /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
[RUN] 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.
Running hooks in /etc/ca-certificates/update.d...
done.

Done: node0_RP0_CPU0


No reachable peer nodes found; only the local node was processed.
```

Current available script:

- **Cisco IOS XR7 (Lindt) Software - https://cisco.app.box.com/s/ccvt1pt1wj7bc9qb16wyb31lrw9wi4je**

On all XR7 aarch64 platforms the remediation will be effective, since enforcement will be introduced only in upcoming releases.

- **Cisco 8000:** 8011-4G24Y4H-I and 8404
- **NCS 540:** N540X-4Z14G2Q-D, N540X-4Z14G2Q-A, N540X-8Z16G-SYS-D, N540X-8Z16G-SYS-A, N540X-6Z18G-SYS-D, N540X-6Z18G-SYS-A, N540-6Z18G-SYS-D N540-6Z18G-SYS-A, N540-6Z14S-SYS-D, N540-8Z12G-SYS-D, N540X-6Z6G-SYS, and N540-FH-AGG-SYS



Tip: Scripts can be tested before execution.

*A dry-run option is available for eXR and XR7 scripts by adding **-n** at the end of the command. It can also be used after executing the script to validate that certificate names where commented and removed.*

<#root>

```
    [node0_RP0_CPU0:/misc/disk1]$
```

./xr7_remove_eMudhra_cert.sh

-n

***** DRY RUN: no changes will be made *****

```
================ LOCAL NODE ================
Node: node0_RP0_CPU0
-- Matching lines in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
```

[DRY-RUN]

```
 sed -i '/Comodo_AAA_Services_root.crt\|emSign_ECC_Root_CA_-_G3.crt/ s/^\([^!]\)/!\1/' /etc/ca-certific
```

[DRY-RUN]

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

[DRY-RUN]

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

[DRY-RUN]

```
 update-ca-certificates
Done: node0_RP0_CPU0
No reachable peer nodes found; only the local node was processed.
```

References

1. Cisco Security Advisory: cisco-sa-emudhra-info-ScS22A1r
2. Cisco Talos Blog: Compromised eMudhra Intermediate Certificates