

# IOS XR 지침 - Mudhra 루트 및 중간 인증 기관에 대한 긴급 불신

## 목차

---

## 소개

인증서 확인 및 교정 단계를 포함하여 Cisco IOS XR 라우터에서 eMudhra 인증서 노출을 식별하고 완화하는 방법을 알아보십시오.

## 배경 정보

이 문서에서는 다음을 포함하여 Cisco IOS XR을 실행하는 Cisco 통신 사업자 라우팅 플랫폼에 대한 운영 지침 및 중간 완화 절차를 제공합니다.

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

이러한 절차에서는 [Cisco Security Advisory cisco-sa-emudhra-info-ScS22A1r](#)에 설명된 대로 손상된 eMudhra Certificate Authority와 관련된 잠재적 노출을 [해결합니다](#).

이 문서에서는 IOS XR Linux 인증서 저장소에서 관련 인증서를 식별하고, 잠재적인 노출을 평가하고, 해당하는 경우 중간 완화 절차를 적용하는 방법에 대해 설명합니다.

## 취약성 및 위협 상황

2026년 10월 17일부터 10월 20일 사이, 2025년 4월 이무드라에서 열린 키생성기념식(KGC)에서 유례없는 암호화 결함이 공개되었다. 키 생성 중 무작위성이 깨져 8개(8개)의 Mudhra 중간 인증 기관(6개 TLS 발급 CA 및 2개 코드 서명 CA)의 개인 키는 몇 초 내에 인증되지 않은 사용자에게 의해 인수 분해되고 파생될 수 있습니다.

핵심 복합 요소(Sectigo 상호 서명): 2025년 5월, 감염된 8개의 모든 중간 CA가 Sectigo 레거시 루트(AAA Certificate Services)에 의해 교차 서명되었습니다. Sectigo의 루트는 공용 및 엔터프라이즈 신뢰 저장소에 유비쿼터스 방식으로 포함되므로, 네이티브 eMudhra 루트가 없는 경우에도 이러한 손상된 중간 CA에서 발급한 인증서는 운영 체제 및 TLS 스택에서 전역적으로 기본적으로 신뢰됩니다.

# Cisco IOS XR 인증서 아키텍처 및 노출 분석

IOS XR 애플리케이션은 기본적으로 XR 인증서 저장소를 사용합니다. IOS XR Linux CA 번들에 포함된 두 개의 Mudhra 인증서가 있습니다. 다음과 같은 경우 세 가지 특정 시나리오에서만 사용됩니다.

- Linux 명령줄은 HTTPS 서버에 대해 curl 또는 wget을 실행하는 데 사용됩니다
- LDAP는 TLS를 통해 액세스
- Opflex 구현(ASR 9000 Series에만 해당)

## 구성된 신뢰 지점 및 인증서 감사 및 식별

26.4.1 이전의 모든 Cisco IOS XR 버전(2026년 11월 30일에 릴리스됨)에는 이러한 CA 인증서가 포함되어 있습니다. 이러한 인증서가 XR 디바이스에 있는지 확인하려면 XR Linux CLI에 액세스하여 certificates.conf 파일의 내용을 확인합니다.

<#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
```

인증서에 하나 또는 두 인증서가 모두 언급되어 있는 경우 두 파일의 경로를 찾습니다.

<#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
```

이러한 파일이 있고 certificates.conf에서 참조되는 경우 디바이스가 악용될 수 있습니다.

## 리미디에이션 절차

완화 단계는 다음과 같습니다.

- ! 모든 certificate.conf 파일의 시작 부분에
- 찾은 인증서 제거
- certificate.conf 파일 업데이트

eXR 릴리스의 경우:

! 모든 certificate.conf 파일의 시작 부분에

<#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
```

찾은 인증서 제거

<#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 파일 업데이트

<#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.
```

이 절차는 간단하지만 모든 VM(모든 노드의 기본 SDR 및 sysadmin)과 라우터의 호스트 OS에서 반복해야 합니다.

이 절차는 셸 스크립트를 실행하여 자동화할 수 있습니다.

- 활성 RP의 관리 VM에 스크립트를 업로드하고 복사합니다.

<#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

- 활성 RP의 관리자 VM으로 이동

<#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:~]\$

- 스크립트 실행

<#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.

모든 VM 및 호스트 OS에서 인증서 이름은 certificates.conf에 코멘트되고, 인증서는 제거 및 업데이트됩니다.

스크립트 링크: <https://cisco.box.com/s/mevtcydjarl2tz0rc39862x100b8x3mu>

XR7 릴리스의 경우:

XR7 릴리스에 대한 절차는 아직 검토 중입니다.

## 참조

1. [Cisco 보안 권고: cisco-sa-emudhra-info-ScS22A1r](#)
2. [Cisco Talos 블로그: 감염된 eMudhra 중간 인증서](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.