

IOS XR-Leitfaden - Misstrauen gegenüber den Behörden für Ausstellungs- und Zwischenzertifikate im Notfall

Inhalt

Einleitung

Erfahren Sie, wie Sie auf Cisco IOS XR-Routern das Risiko von Mudhra-Zertifikaten erkennen und reduzieren können, einschließlich Zertifikatprüfungen und Sanierungsmaßnahmen.

Hintergrundinformationen

Dieses Dokument enthält betriebliche Anleitungen und Zwischenverfahren zur Risikominimierung für Cisco Service Provider-Routing-Plattformen mit Cisco IOS XR. Dazu gehören:

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

Diese Verfahren gehen auf potenzielle Risiken im Zusammenhang mit den kompromittierten Mudhra-Zertifizierungsstellen ein, wie in [Cisco Security Advisory cisco-sa-emudhra-info-ScS22A1r](#) dokumentiert.

Der Artikel erläutert, wie relevante Zertifikate im IOS XR Linux-Zertifikatspeicher identifiziert, potenzielle Risiken bewertet und ggf. vorläufige Eindämpfungsverfahren angewendet werden.

Kontext zu Schwachstellen und Bedrohungen

Zwischen dem 17. Oktober und dem 20. Oktober 2026 wurde ein beispielloser kryptographischer Defekt bei der Schlüsselgenerierungszeremonie (Key Generation Ceremony, KGC) im April 2025 in Mudhra öffentlich bekannt gegeben. Aufgrund der fehlerhaften Zufälligkeit während der Schlüsselgenerierung können die privaten Schlüssel für acht (8) Mudhra Intermediate Certificate Authorities (6 TLS Issuing CAs und 2 Code Signing CAs) innerhalb von Sekunden faktorisiert und von nicht autorisierten Akteuren abgeleitet werden.

Kritischer Compoundierungsfaktor (Sectio-Kreuzsignatur): Im Mai 2025 wurden alle acht kompromittierten Zwischen-CAs von Sectigo Legacy Root (AAA Certificate Services) quersigniert. Da der Root von Sectigo allgegenwärtig in öffentlichen und Enterprise Trust Stores eingebettet ist, werden von diesen kompromittierten zwischengeschalteten CAs ausgestellte Zertifikate standardmäßig global auf allen Betriebssystemen und TLS-Stacks als vertrauenswürdig angesehen, selbst wenn der native Mudhra-Root nicht vorhanden ist.

Architektur des Cisco IOS XR-Zertifikats und Belichtungsanalyse

IOS XR-Anwendungen verwenden standardmäßig den XR-Zertifikatspeicher. Im IOS XR Linux-CA-Paket sind zwei Mudhra-Zertifikate enthalten. Sie werden nur in drei spezifischen Szenarien verwendet, wenn:

- Die Linux-Befehlszeile wird verwendet, um curl oder wget gegen einen HTTPS-Server auszuführen
- LDAP wird über TLS genutzt
- OpFlex ist implementiert (nur für ASR der Serie 9000)

Prüfen und Identifizieren konfigurierter Vertrauenspunkte und Zertifikate

Jede Cisco IOS XR-Version vor 26.4.1 (Veröffentlichung am 30.11.2026) enthält diese Zertifizierungsstellenzertifikate. Um zu überprüfen, ob diese Zertifikate auf einem XR-Gerät vorhanden sind, rufen Sie die XR Linux-CLI auf, und überprüfen Sie den Inhalt der Datei "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
```

Wenn ein oder beide Zertifikate in den Zertifikaten angegeben sind, suchen Sie nach dem Pfad der beiden Dateien:

```
<#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
```

Wenn diese Dateien vorhanden sind und in Certificates.conf referenziert werden, könnte Ihr Gerät ausgenutzt werden.

Sanierungsverfahren

Folgende Schritte zur Risikominimierung sind erforderlich:

- Fügen Sie eine ! am Anfang jeder certificate.conf-Datei
- gefundene Zertifikate entfernen
- Datei certificate.conf aktualisieren

Für eXR-Versionen:

Hinzufügen eines ! am Anfang jeder certificate.conf-Datei

```
<#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
```

Gefundene Zertifikate entfernen

```
<#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-Datei aktualisieren

```
<#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.
```

Obwohl dieses Verfahren am Ende einfach ist, muss es auf jedem VM (default-sdr und sysadmin für jeden Knoten) und dem Host-Betriebssystem des Routers wiederholt werden.

Dieses Verfahren kann durch Ausführen eines Shell-Skripts automatisiert werden:

- Laden Sie das Skript hoch, und kopieren Sie es in die virtuelle Admin-Maschine auf dem aktiven 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

- Rufen Sie die Admin-VM des aktiven RP auf.

<#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:~]\$

- Skript ausführen

<#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.
```

Auf allen VMs und Host-Betriebssystemen werden die Zertifikatsnamen auf `certificats.conf` kommentiert, die Zertifikate werden entfernt und aktualisiert.

Skript-Link: <https://cisco.box.com/s/mevtcydjarl2tz0rc39862x100b8x3mu>

Für XR7-Versionen:

Das Verfahren für XR7-Releases wird derzeit noch überprüft.

Referenzen

1. [Cisco Sicherheitsempfehlungen: cisco-sa-emudhra-info-ScS22A1r](#)
2. [Cisco Talos-Blog: Kompromittierte Mudhra-Zwischenzertifikate](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.