

Guide IOS XR - Méfiance d'urgence des autorités de certification racine et intermédiaire eMudhra

Table des matières

Introduction

Découvrez comment identifier et limiter l'exposition aux certificats eMudhra sur les routeurs Cisco IOS XR, y compris les vérifications de certificats et les étapes de correction.

Informations générales

Ce document fournit des conseils opérationnels et des procédures d'atténuation provisoires pour les plates-formes de routage Cisco Service Provider exécutant Cisco IOS XR, notamment :

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

Ces procédures concernent l'exposition potentielle associée aux autorités de certification eMudhra compromises, comme indiqué dans le [document Cisco Security Advisory cisco-sa-emudhra-info-ScS22A1r](#).

L'article explique comment identifier les certificats pertinents dans le magasin de certificats IOS XR Linux, évaluer l'exposition potentielle et appliquer des procédures d'atténuation provisoires, le cas échéant.

Vulnérabilité et contexte de menace

Entre le 17 et le 20 octobre 2026, un défaut cryptographique sans précédent a été révélé lors de la cérémonie de génération de clés (KGC) d'avril 2025 à Mehmudhra. En raison du caractère aléatoire cassé lors de la génération de clé, les clés privées de huit (8) autorités de certification intermédiaires eMudhra (6 AC émettrices de TLS et 2 AC de signature de code) peuvent être factorisées et dérivées par des acteurs non autorisés en quelques secondes.

Facteur de préparation critique (signature croisée de section) : En mai 2025, les huit AC intermédiaires compromises ont été signées par Sectigo legacy root (AAA Certificate Services). Comme la racine de Sectigo est omniprésente dans les magasins de confiance publics et d'entreprise, les certificats émis par ces CA intermédiaires compromis sont approuvés par défaut sur les systèmes d'exploitation et les piles TLS dans le monde entier, même si la racine eMudhra native est absente.

Architecture de certificat Cisco IOS XR et analyse de l'exposition

Les applications IOS XR utilisent par défaut le magasin de certificats XR. Deux certificats eMudhra sont inclus dans l'offre groupée IOS XR Linux CA. Ils ne sont utilisés que dans trois scénarios spécifiques, lorsque :

- La ligne de commande Linux est utilisée pour exécuter curl ou wget sur un serveur HTTPS
- LDAP est accessible via TLS
- Opflex est mis en oeuvre (uniquement sur la gamme ASR 9000)

Audit et identification des certificats et des points de confiance configurés

Toute version de Cisco IOS XR antérieure à 26.4.1 (à paraître le 30 novembre 2026) contient ces certificats CA. Pour vérifier que ces certificats sont présents sur un périphérique XR, accédez à l'interface de ligne de commande de XR Linux et vérifiez le contenu du fichier 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
```

Si un ou les deux certificats sont mentionnés sur les certificats présents, recherchez le chemin d'accès des deux fichiers :

```
<#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
```

Si ces fichiers sont présents et sont référencés dans `certificates.conf`, votre périphérique peut être exploité.

Procédures de correction

Les étapes d'atténuation comprennent :

- ajoutez un `!` au début de chaque fichier `certificate.conf`
- supprimer les certificats trouvés
- mettre à jour le fichier `certificate.conf`

Pour les versions eXR :

Ajouter un `!` au début de chaque fichier `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
```

Supprimer les certificats trouvés

<#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
```

Mettre à jour le fichier `certificate.conf`

<#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.
```

Bien que cette procédure soit simple, elle doit être répétée sur chaque machine virtuelle (default-sdr et sysadmin pour chaque noeud) et sur le système d'exploitation hôte du routeur.

Cette procédure peut être automatisée en exécutant un script shell :

- Téléchargez et copiez le script sur la machine virtuelle admin sur le RP actif

```
<#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
```

- Accéder à la machine virtuelle admin du RP actif

```
<#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:~]$
```

- Exécuter le 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.
```

Sur toutes les machines virtuelles et tous les systèmes d'exploitation hôtes, les noms de certificat seront commentés sur certificates.conf, les certificats seront supprimés et mis à jour.

Lien du script : <https://cisco.box.com/s/mevtcydjarl2tz0rc39862x100b8x3mu>

Pour les versions XR7 :

La procédure pour les versions XR7 est toujours en cours d'examen.

Références

1. [Avis de sécurité Cisco : cisco-sa-emudhra-info-ScS22A1r](#)
2. [Blog Cisco Talos : Certificats intermédiaires eMudhra compromis](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.