

Orientação IOS XR - Desconfiança de Emergência da Raiz de Mudhra e Autoridades de Certificação Intermediárias

Contents

Introdução

Saiba como identificar e mitigar a exposição ao certificado Mudhra em roteadores Cisco IOS XR, incluindo verificações de certificado e etapas de correção.

Informações de Apoio

Este documento fornece orientação operacional e procedimentos de mitigação provisórios para as plataformas de roteamento do Cisco Service Provider executando o Cisco IOS XR, incluindo:

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

Esses procedimentos abordam a exposição potencial associada às Autoridades de Certificação de Mudhra comprometidas, conforme documentado no [Cisco Security Advisory cisco-sa-emudhra-info-ScS22A1r](#).

O artigo explica como identificar certificados relevantes no armazenamento de certificados IOS XR Linux, avaliar a exposição potencial e aplicar procedimentos de mitigação provisórios onde aplicável.

Vulnerabilidade e contexto de ameaça

Entre 17 de outubro e 20 de outubro de 2026, um defeito criptográfico sem precedentes na cerimônia de geração de chaves (KGC) de abril de 2025 em Mudhra foi divulgado publicamente. Devido à aleatoriedade quebrada durante a geração de chave, as chaves privadas de oito (8) Autoridades de Certificação Intermediárias de Mudhra (6 CAs Emissoras de TLS e 2 CAs de Assinatura de Código) podem ser fatoradas e derivadas por agentes não autorizados em segundos.

Fator De Composição Crítico (Assinatura Cruzada De Sectigo): Em maio de 2025, todas as oito CAs intermediárias comprometidas foram assinadas pela raiz legada da Sectigo (AAA Certificate Services). Como a raiz da Sectigo está onipresente em lojas de confiança públicas e corporativas, os certificados emitidos por essas CAs intermediárias comprometidas são confiáveis por padrão em todos os sistemas operacionais e pilhas TLS globalmente, mesmo que a raiz nativa da Mudhra esteja ausente.

Arquitetura de certificado e análise de exposição do Cisco IOS XR

Os aplicativos IOS XR usam, por padrão, o armazenamento de certificados XR. Há dois certificados Mudhra incluídos no pacote IOS XR Linux CA. Eles são usados apenas em três cenários específicos, quando:

- A linha de comando do Linux é usada para executar curl ou wget em um servidor HTTPS
- LDAP é acessado por TLS
- O Opflex é implementado (somente no ASR 9000 Series)

Auditar e identificar pontos de confiança e certificados configurados

Qualquer versão do Cisco IOS XR anterior à 26.4.1 (a ser lançada em 30 de novembro de 2026) contém esses certificados CA. Para validar se esses certificados estão presentes em um dispositivo XR, acesse a CLI do Linux XR e verifique o conteúdo do arquivo 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
```

Se um ou ambos os certificados forem mencionados nos certificados presentes, procure o caminho de ambos os arquivos:

```
<#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
```

Se esses arquivos estiverem presentes e forem mencionados no certificates.conf, o dispositivo poderá ser explorado.

Procedimentos de correção

As etapas de mitigação consistem em:

- adicionar um ! no início de cada arquivo certificate.conf
- remover certificados encontrados
- atualizar arquivo certificate.conf

Para versões eXR:

Adicione um ! no início de cada arquivo 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
```

Remover certificados encontrados

```
<#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
```

Atualizar arquivo 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.
```

Embora, esse procedimento acabe sendo simples, mas precisa ser repetido em cada VM (default-sdr e sysadmin para cada nó) e no SO do host do roteador.

Este procedimento pode ser automatizado executando-se um script de shell:

- Carregue e copie o script para a VM admin no RP ativo

<#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

- Vá para admin VM do RP ativo

<#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:~]\$

- Executar o 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.
```

Em todas as VMs e sistemas operacionais de host, os nomes de certificados serão comentados no `certificates.conf`, os certificados serão removidos e atualizados.

Link do script: <https://cisco.box.com/s/mevtcydjarl2tz0rc39862x100b8x3mu>

Para versões XR7:

O procedimento para as versões XR7 ainda está em revisão.

Referências

1. [Consultivo de segurança Cisco: cisco-sa-emudhra-info-ScS22A1r](#)
2. [Blog do Cisco Talos: Certificados intermediários de Mudhra comprometidos](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.