

IOS XR指南 — 紧急不信任根证书颁发机构和中间证书颁发机构

目录

简介

了解如何识别和缓解Cisco IOS XR路由器上的Mudhra证书风险，包括证书检查和补救步骤。

背景信息

本文档为运行Cisco IOS XR的思科服务提供商路由平台提供操作指南和临时缓解程序，包括：

- Cisco ASR 9000系列
- Cisco 8000 系列
- 思科NCS 1000系列
- 思科NCS 4000系列
- 思科NCS 5500系列
- 思科NCS 6000系列
- 思科NCS 540/560系列
- 思科XRv 9000

这些步骤可解决与eMudhra Certificate Authorities相关的潜在风险，如[Cisco Security Advisory cisco-sa-emudhra-info-ScS22A1r中所述](#)。

本文解释如何在IOS XR Linux证书存储中识别相关证书、评估潜在风险，并在适用时应用临时缓解程序。

漏洞和威胁情景

在2026年10月17日至10月20日之间，在2025年4月的密钥生成仪式(Key Generation Certification, KGC)中，一个前所未有的密码缺陷被公开披露。由于在密钥生成期间出现中断的随机性，八(8)个Mudhra中间证书颁发机构（6个TLS颁发CA和2个代码签名CA）的私钥可在数秒内被非授权参与者分解和导出。

关键综合因素（Sectigo交叉签名）：2025年5月，所有八个受侵害的中间CA都由Sectigo传统根（AAA证书服务）交叉签名。由于Sectigo的根通常嵌入在公共信任库和企业信任库中，因此默认情况下，即使没有本地Mudhra根，这些受感染的中间CA颁发的证书也可在全局的操作系统和TLS堆栈中受信任。

思科IOS XR证书架构和风险分析

IOS XR应用程序默认使用XR证书存储。IOS XR Linux CA捆绑包中包含两个eMudra证书。它们仅在以下三种特定情况下使用：

- Linux命令行用于对HTTPS服务器运行curl或wget
- 通过TLS访问LDAP
- 实施Opflex (仅在ASR 9000系列上)

审核并确定配置的信任点和证书

26.4.1 (将于2026年11月30日发布) 之前的任何Cisco IOS XR版本都包含这些CA证书。要验证XR设备上是否存在这些证书，请访问XR Linux CLI并验证certificates.conf文件的内容：

<#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

如果证书中提及一个或两个证书，则查找这两个文件的路径：

<#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

如果这些文件存在，并且在certificates.conf中引用，则您的设备可能遭到攻击。

补救程序

缓解步骤包括：

- 添加！在每个certificate.conf文件的开头
- 删除找到的证书
- 更新certificate.conf文件

对于eXR版本：

添加！在每个certificate.conf文件的开头

```
<#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
```

删除找到的证书

```
<#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
```

更新certificate.conf文件

```
<#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.
```

尽管此过程最终很简单，但需要在每个VM（每个节点的default-sdr和sysadmin）和路由器的主机操作系统上重复此过程。

可以通过运行shell脚本自动执行此过程：

- 将脚本上传并复制到活动RP上的管理VM

```
<#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

- 转到活动RP的管理虚拟机

<#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:~]\$

- 执行脚本

<#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.

在所有VM和主机操作系统上，证书名称将在certificates.conf上获得注释，证书将被删除并更新。

脚本链接：<https://cisco.box.com/s/mevtcydjarl2tz0rc39862x100b8x3mu>

对于XR7版本：

XR7版本的程序仍在审核中。

参考

1. [Cisco安全建议:cisco-sa-emudhra-info-ScS22A1r](#)
2. [Cisco Talos博客：受感染的Mudhra中间证书](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。