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软件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 8000 系列
- Cisco ASR 9000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/

```
/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。

传统IOS XR版本（32位）不受此问题的影响。

补救程序

缓解步骤包括：

- 在前面加上“！”到certificate.conf文件中包含受影响证书的每一行的开头
- 删除找到的证书
- 更新和同步系统范围的SSL/TLS证书

对于eXR版本

在前面加上“！”到certificate.conf文件中包含受影响证书的每一行的开头

<#root>

```
    [xr-vm_node0_RP0_CPU0:~]$
```

sed -i -E '/Comodo_AAA_Services_root\.crt|emSign_ECC_Root_CA_-_G3\.crt/s/^/!/' /etc/ca-certificates.conf

```
[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
```

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

更新和同步系统范围的SSL/TLS证书

<#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。然后访问管理VM的Linux CLI（对于NCS 560路由器，必须在XR VM Linux CLI上执行脚本）

<#root>

```
    sysadmin-vm:0_RP0#
```

copy harddisk:asr9k_remove_eMudhra_cert.sh location 0/RP0/CPU0/VM1 harddisk:

```
Tue Oct 27 01:59:29.149 UTC+00:00
Copying harddisk:asr9k_remove_eMudhra_cert.sh to harddisk:
asr9k_remove_eMudhra_cert.sh 100% 2410 2.4KB/s 00:00
```

File copied successfully

```
sysadmin-vm:0_RP0#
sysadmin-vm:0_RP0#
```

run

[sysadmin-vm:0_RP0:~]$

添加执行权限并运行脚本

<#root>

[sysadmin-vm:0_RP1:~]$

chmod +x asr9k_remove_eMudhra_cert.sh

[sysadmin-vm:0_RP0:~]$

./asr9k_remove_eMudhra_cert.sh

===== local node (this XR VM) =====

-- Entries found in /etc/ca-certificates.conf:

mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt

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.

Running hooks in /etc/ca-certificates/update.d...

asr9k_remove_eMudhra_cert.sh

===== lc0_admin =====

```
-- Entries found in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.
```

===== lc0_xr =====

```
-- Entries found in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.
```

===== my_host =====

```
-- Entries found in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.
```

===== rsp0_xr =====

```
-- Entries found in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.
```

===== rsp1_admin =====

```
-- Entries found in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.

===== rsp1_xr =====


-- Entries found in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
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.
Running hooks in /etc/ca-certificates/update.d...
done.
```

在管理员VM可以访问的所有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。

当前可用的脚本有：

- ASR 9000路由器系列 — https://cisco.app.box.com/file/2557835175620?s=tmogb804gb75pdy2nrivm9jfp84ybqyt
- NCS 540和5500路由器系列 — https://cisco.app.box.com/file/2557840859193?s=1t79efmqk8g3ppnyoegmt5iu6q0xps01
- NCS 560路由器系列 — https://cisco.app.box.com/s/co7k52pwayjs7nx1toyse0g56a34gnrd

如果脚本执行挂起，则一个或多个主机可能提示输入密码。在这种情况下，请手动执行补救程序。

对于XR7版本

思科IOS XR7软件使用SELinux，并且已在以下版本中的不同平台上启用实施：

- 思科8000(x86_64):24.4.1中启用了实施
- NCS 540L:26.1.1中启用了实施
- NCS 5700:26.2.1中启用了实施
- NCS 1000(Lindt):26.3.1中启用了实施

验证实施状态。如果返回Permissive，则可以执行手动补救或脚本。如果返回Enforcing（实施），请升级到26.4.1版本。

<#root>

RP/0/RP0/CPU0:

Router-1

#

run

[node0_RP0_CPU0:~]$

getenforce

Enforcing

RP/0/RP0/CPU0:

Router-2

#

run

[node0_RP0_CPU0:~]$

getenforce

Permissive

将脚本上传到活动RP。然后访问Linux CLI并切换到硬盘目录

<#root>

RP/0/RP0/CPU0:Router#

run

[node0_RP0_CPU0:~]$

```
cd /misc/disk1

[node0_RP0_CPU0:/misc/disk1]$
```

添加执行权限并运行脚本

<#root>

```
    [node0_RP0_CPU0:/misc/disk1]$

chmod +x xr7_remove_eMudhra_cert.sh

[node0_RP0_CPU0:/misc/disk1]$

./xr7_remove_eMudhra_cert.sh

================ LOCAL NODE ================
Node: node0_RP0_CPU0
-- Matching lines in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt
[RUN] prepend '!' to matching lines in /etc/ca-certificates.conf
[RUN] rm -f /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt
[RUN] rm -f /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
[RUN] 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.
Running hooks in /etc/ca-certificates/update.d...
done.

Done: node0_RP0_CPU0

No reachable peer nodes found; only the local node was processed.
```

当前可用的脚本：

- 思科IOS XR7(Lindt)软件 — https://cisco.app.box.com/s/ccvt1pt1wj7bc9qb16wyb31lrw9wi4je

在所有XR7 aarch64平台上，补救将有效，因为实施将仅在即将发布的版本中引入。

- Cisco 8000 ：8011-4G24Y4H-I和8404
- NCS 540:N540X-4Z14G2Q-D、N540X-4Z14G2Q-A、N540X-8Z16G-SYS-D、N540X-8Z16G-SYS-A、N540X-6Z18G-SYS-D、N540X-6Z18G sys-A、N540-6Z18G-SYS-D、N540-6Z18G-SYS-A、N540-6Z14S-SYS-D、N540-8Z12G-SYS-D、N540X-6Z6G-SYS和N540-FH-AGG-SYS



提示：脚本可以在执行之前进行测试。

通过在命令末尾添加 — n，可以为eXR和XR7脚本提供干燥运行选项。它也可以在执行脚本后用于验证证书名称，该名称被注释和删除。

<#root>

```
    [node0_RP0_CPU0:/misc/disk1]$

./xr7_remove_eMudhra_cert.sh



-n



*** DRY RUN: no changes will be made ***


================ LOCAL NODE ================
Node: node0_RP0_CPU0
-- Matching lines in /etc/ca-certificates.conf:
mozilla/Comodo_AAA_Services_root.crt
mozilla/emSign_ECC_Root_CA_-_G3.crt

[DRY-RUN]

 sed -i '/Comodo_AAA_Services_root.crt\|emSign_ECC_Root_CA_-_G3.crt/ s/^\([^!]\)/!\1/' /etc/ca-certific

[DRY-RUN]

 rm -f /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt

[DRY-RUN]

 rm -f /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
```

```
[DRY-RUN]

 update-ca-certificates
Done: node0_RP0_CPU0
No reachable peer nodes found; only the local node was processed.
```

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）。