

IOS XR指南 — 緊急不信任Mudhra根和中間證書頒發機構

目錄

簡介

瞭解如何識別和緩解Cisco IOS XR路由器上的eMudra證書風險，包括證書檢查和補救步驟。

背景資訊

本檔案為執行Cisco IOS XR的思科服務供應商路由平台提供運作指引和臨時緩解程序，包括：

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

這些程式可解決與eMudhra Certificate Authorities相關的潛在風險，如[思科安全諮詢cisco-sa-emudhra-info-ScS22A1r中所述](#)。

本文說明如何在IOS XR Linux證書儲存中識別相關證書、評估潛在風險，並在適用時應用臨時緩解程式。

漏洞和威脅情景

在2026年10月17日至10月20日期間，在2025年4月的eMudhra金鑰生成儀式(KGC)中一個前所未有的密碼缺陷被公開披露。由於金鑰生成期間出現中斷的隨機性，八(8)個中間證書頒發機構(6個TLS頒發CA和2個代碼簽名CA)的私鑰可由未經授權的參與者在幾秒鐘內分解和匯出。

關鍵複合因素 (Sectigo交叉簽名)：2025年5月，所有八個受危害的中間CA均由Sectigo舊版根(AAA憑證服務)交叉。由於Sectigo的根目錄普遍嵌入在公共信任儲存區和企業信任儲存區中，因此預設情況下，即使沒有本機eMudhra根，這些受感染的中間CA頒發的證書也可在全域性的作業系統和TLS堆疊中受信任。

Cisco IOS XR憑證架構和曝光度分析

預設情況下，IOS XR應用程式使用XR證書儲存。IOS XR Linux CA捆綁包中包含兩個eMudra證書

。它們僅在以下三種特定情況下使用：

- Linux命令列用於對HTTPS伺服器運行curl或wget
- 通過TLS訪問LDAP
- 實施Opflex (僅在ASR 9000系列上)

稽核並確定配置的信任點和證書

26.4.1之前的任何Cisco IOS XR版本 (將於2026年11月30日發佈) 都包含這些CA證書。要驗證XR裝置上是否存在這些證書，請訪問XR Linux CLI並驗證certificates.conf檔案的內容：

<#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

如果憑證上提到其中一個或兩個憑證，請尋找兩個檔案的路徑：

<#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

如果這些檔案存在，並且在certificates.conf中引用，則您的裝置可能會被攻擊。

補救程式

緩解步驟包括：

- 新增！在每個certificate.conf檔案的開始位置
- 刪除找到的證書
- update certificate.conf檔案

對於eXR版本：

新增！在每個certificate.conf檔案的開始位置

<#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
```

刪除找到的證書

<#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檔案

<#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.
```

雖然此過程最終非常簡單，但需要在每個VM（每個節點的default-sdr和sysadmin）和路由器的主機OS上重複此過程。

可以通過運行shell指令碼來自動執行此過程：

- 將指令碼上傳並複製到活動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

- 轉到活動RP的管理虛擬機器

<#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:~]\$

- 執行指令碼

<#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和主機作業系統上，證書名稱將在certificates.conf上得到評論，證書將被刪除並更新。

指令碼連結：<https://cisco.box.com/s/mevtcydjarl2tz0rc39862x100b8x3mu>

對於XR7版本：

XR7版本的操作過程仍在稽核中。

參考資料

1. [思科資安顧問諮詢：cisco-sa-emudhra-info-ScS22A1r](#)
2. [Cisco Talos部落格：遭破壞的Mudra中間憑證](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。