

Linee guida di IOS XR - Emergenza diffidenza verso le autorità radice e intermedie dei certificati di eMudhra

Sommario

Introduzione

Scopri come identificare e ridurre l'esposizione ai certificati eMudhra sui router Cisco IOS XR, tra cui i controlli dei certificati e le procedure di monitoraggio e aggiornamento.

Premesse

Questo documento offre linee guida operative e procedure provvisorie di mitigazione per le piattaforme di routing di Cisco Service Provider che eseguono Cisco IOS XR, tra cui:

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

Queste procedure affrontano il potenziale di esposizione associato alle autorità di certificazione eMudhra compromesse, come documentato in [Cisco Security Advisory cisco-sa-emudhra-info-ScS22A1r](#).

L'articolo spiega come identificare i certificati pertinenti nell'archivio certificati di IOS XR Linux, valutare l'esposizione potenziale e applicare procedure di mitigazione provvisorie, se applicabili.

Vulnerabilità e contesto di minaccia

Tra il 17 e il 20 ottobre 2026, un difetto crittografico senza precedenti nella cerimonia di Key Generation (KGC) a Mudhra dell'aprile 2025 è stato reso pubblico. A causa di casualità interrotta durante la generazione della chiave, le chiavi private per otto (8) Autorità di certificazione intermedie eMudhra (6 autorità di certificazione che rilasciano TLS e 2 autorità di certificazione che firmano il codice) possono essere fattorizzate e derivate da attori non autorizzati in pochi secondi.

Fattore di composizione critico (firma incrociata sezione): Nel maggio 2025, tutte e otto le CA intermedie compromesse sono state controfirmate da Sectigo legacy root (AAA Certificate Services). Poiché la radice di Sectigo è ubiquitativamente incorporata in archivi trust pubblici ed aziendali, i certificati emessi da queste CA intermedie compromesse sono considerati attendibili per impostazione predefinita in tutti i sistemi operativi e stack TLS a livello globale, anche se la radice eMudhra nativa è assente.

Architettura dei certificati Cisco IOS XR e analisi dell'esposizione

Per impostazione predefinita, le applicazioni IOS XR utilizzano l'archivio certificati XR. Nel bundle CA di IOS XR Linux sono inclusi due certificati eMudhra. Vengono utilizzati solo in tre scenari specifici, quando:

- La riga di comando Linux viene utilizzata per eseguire curl o wget su un server HTTPS
- Accesso a LDAP tramite TLS
- Opflex è implementato (solo su ASR serie 9000)

Verifica e identificazione di trust e certificati configurati

Qualsiasi versione di Cisco IOS XR precedente alla 26.4.1 (disponibile dal 30 novembre 2026) contiene questi certificati CA. Per verificare che questi certificati siano presenti su un dispositivo XR, accedere alla CLI di XR Linux e verificare il contenuto del file 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 nei certificati sono presenti uno o entrambi i certificati, cercare il percorso di entrambi i file:

```
<#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 questi file sono presenti e vi viene fatto riferimento in certificates.conf, il dispositivo potrebbe essere sfruttato.

Procedure di risoluzione

Le fasi di mitigazione consistono in:

- aggiungi un ! all'inizio di ogni file certificate.conf
- rimuovere i certificati trovati
- aggiornare il file certificate.conf

Per le release di eXR:

Aggiungi un ! all'inizio di ogni file 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
```

Rimuovi certificati trovati

```
<#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
```

Aggiorna file 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.

Questa procedura risulta tuttavia semplice, ma deve essere ripetuta su ogni VM (default-sdr e sysadmin per ogni nodo) e sul sistema operativo host del router.

Questa procedura può essere automatizzata eseguendo uno script shell:

- Caricare e copiare lo script nella VM di amministrazione sull'RP attivo

```
<#root>
```

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

```
copy hddisk:exr_remove_eMudhra_cert.sh hddisk: location 0/RP0/CPU0/VM1
```

```
Tue Oct 27 01:59:29.149 UTC+00:00
```

```
Copying hddisk:exr_remove_eMudhra_cert.sh to hddisk:
```

```
exr_remove_eMudhra_cert.sh 100% 1604 4.3MB/s 00:00
```

```
File copied successfully
```

- Passare alla VM di amministrazione dell'RP attivo

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

- Eseguire lo 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.
```

In tutte le macchine virtuali e in tutti i sistemi operativi host i nomi dei certificati verranno commentati in certificates.conf e i certificati verranno rimossi e aggiornati.

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

Per le release XR7:

La procedura per le versioni XR7 è ancora in fase di revisione.

Riferimenti

1. [Cisco Security Advisory: cisco-sa-emudhra-info-ScS22A1r](#)
2. [Cisco Talos Blog: Certificati eMudhra intermedi compromessi](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).