

# Risoluzione dei problemi di IOS XR 30 settembre 2021 - Scadenza certificato CA X3 radice DST

## Sommario

[Introduzione](#)

[Esempio di certificato](#)

[Prima del 30 settembre 2021](#)

[Il 30 settembre 2021 e dopo](#)

[Messaggi di scadenza certificati](#)

[Soluzione alternativa](#)

[Pre-scadenza](#)

[Post-scadenza](#)

[Soluzione](#)

## Introduzione

Questo documento descrive il significato della scadenza del certificato predefinito 'DST Root CA X3' del 30 settembre 2021 e qualsiasi azione necessaria per risolvere il problema. Nella maggior parte dei casi non è necessaria alcuna azione immediata.

Una comunicazione esterna dell'editore CA radice è disponibile qui:

<https://letsencrypt.org/docs/dst-root-ca-x3-expiration-september-2021/>

## Esempio di certificato

```
RP/0/RP0/CPU0:NCS-5516-A#show crypto ca trustpool
Fri Oct 1 00:00:35.206 UTC
```

```
Trustpool: Built-In
```

```
=====
```

```
CA certificate
```

```
Serial Number : 5F:F8:7B:28:2B:54:DC:8D:42:A3:15:B5:68:C9:AD:FF
```

```
Subject:
```

```
CN=Cisco Root CA 2048,O=Cisco Systems
```

```
Issued By :
```

```
CN=Cisco Root CA 2048,O=Cisco Systems
```

```
Validity Start : 20:17:12 UTC Fri May 14 2004
```

```
Validity End : 20:25:42 UTC Mon May 14 2029
```

```
SHA1 Fingerprint:
```

```
DE990CED99E0431F60EDC3937E7CD5BF0ED9E5FA
```

```
Trustpool: Built-In
```

```
=====
```

```
CA certificate
```

```
Serial Number : 2E:D2:0E:73:47:D3:33:83:4B:4F:DD:0D:D7:B6:96:7E
```

```
Subject:
```

```
CN=Cisco Root CA M1,O=Cisco
```

```
Issued By :
```

```
CN=Cisco Root CA M1,O=Cisco
```

Validity Start : 21:50:24 UTC Tue Nov 18 2008  
Validity End : 21:59:46 UTC Fri Nov 18 2033  
SHA1 Fingerprint:  
45AD6BB499011BB4E84E84316A81C27D89EE5CE7

Trustpool: Built-In

=====  
CA certificate  
Serial Number : 44:AF:B0:80:D6:A3:27:BA:89:30:39:86:2E:F8:40:6B  
Subject:  
CN=DST Root CA X3,O=Digital Signature Trust Co.  
Issued By :  
CN=DST Root CA X3,O=Digital Signature Trust Co.  
Validity Start : 21:12:19 UTC Sat Sep 30 2000  
Validity End : 14:01:15 UTC Thu Sep 30 2021  
SHA1 Fingerprint:  
DAC9024F54D8F6DF94935FB1732638CA6AD77C13

Trustpool: Built-In

=====  
CA certificate  
Serial Number : 3C:91:31:CB:1F:F6:D0:1B:0E:9A:B8:D0:44:BF:12:BE  
Subject:  
OU=Class 3 Public Primary Certification Authority,O=VeriSign\, Inc.,C=US  
Issued By :  
OU=Class 3 Public Primary Certification Authority,O=VeriSign\, Inc.,C=US  
Validity Start : 00:00:00 UTC Mon Jan 29 1996  
Validity End : 23:59:59 UTC Wed Aug 02 2028  
SHA1 Fingerprint:  
A1DB6393916F17E4185509400415C70240B0AE6B

Trustpool: Built-In

=====  
CA certificate  
Serial Number : 05:09  
Subject:  
CN=QuoVadis Root CA 2,O=QuoVadis Limited,C=BM  
Issued By :  
CN=QuoVadis Root CA 2,O=QuoVadis Limited,C=BM  
Validity Start : 18:27:00 UTC Fri Nov 24 2006  
Validity End : 18:23:33 UTC Mon Nov 24 2031  
SHA1 Fingerprint:  
CA3AFBCF1240364B44B216208880483919937CF7

## Prima del 30 settembre 2021

Prima del 30 settembre 2021 gli utenti possono ottenere un messaggio di registro che indica che un certificato sta per scadere, ad esempio

%SECURITY-PKI-6-ERR\_1\_PARAM : CA certificate to be expired in 480 days

È possibile continuare a visualizzare questo messaggio di registro fino alla scadenza del certificato con un conto alla rovescia per il numero di giorni.

Se i 480 giorni sono errati, moltiplicati per 24 ore per errore, il problema è risolto nell'ID bug Cisco [CSCvz62603](#).

ad esempio  $480/24 = 20$  giorni.

## Il 30 settembre 2021 e dopo

Questo certificato non viene utilizzato e non causa alcun impatto sul traffico di produzione o sui servizi di crittografia quando la scadenza è stata testata in laboratorio.

### Messaggi di scadenza certificati

A seconda della versione del codice in uso, è possibile visualizzare alcuni messaggi di scadenza diversi:

```
RP/0/RP0/CPU0:Oct 1 00:06:13.572 UTC: syslog_dev[113]: cepki[261] PID-7101: % CA certificate is not yet valid or has expired.
RP/0/RP0/CPU0:Oct 1 00:06:13.572 UTC: syslog_dev[113]: cepki[261] PID-7101: % Make sure the clock is synchronized with CA's clock.
RP/0/RP0/CPU0:Oct 1 00:06:13.572 UTC: cepki[261]: %SECURITY-PKI-1-CACERT_NOT_VALID : Failed to add CA certificate with subject name /O=Digital Signature Trust Co./CN=DST Root CA X3 to trustpool because certificate has expired or is not yet valid
RP/0/RP0/CPU0:Oct 1 00:06:14.054 UTC: cepki[261]: %SECURITY-CEPKI-6-KEY_INFO : One or more host keypairs exist. Not auto-generating keypairs.
```

Questi messaggi possono essere visualizzati in qualsiasi momento in cui il processo cepki viene riavviato o il router viene ricaricato/il processore di routing (RP) viene avviato.

## Soluzione alternativa

- Per disattivare i messaggi syslog, è possibile configurarli in modo che vengano eliminati, come illustrato nell'esempio.
- Non è necessario installare il certificato sostitutivo, poiché non vi è alcun impatto dalla scadenza del certificato.

### Pre-scadenza

```
%SECURITY-PKI-6-ERR_1_PARAM : CA certificate to be expired in 480 days
```

```
logging suppress rule PRE_CERT_EXPIRY
alarm SECURITY PKI ERR_1_PARAM
!
logging suppress apply rule PRE_CERT_EXPIRY
all-of-router
!
```

### Post-scadenza

```
RP/0/RP0/CPU0:Oct 1 00:06:13.572 UTC: cepki[261]: %SECURITY-PKI-1-CACERT_NOT_VALID : Failed to add CA certificate with subject name /O=Digital Signature Trust Co./CN=DST Root CA X3 to trustpool because certificate has expired or is not yet valid
```

```
logging suppress rule POST_CERT_EXPIRY
alarm SECURITY PKI CACERT_NOT_VALID
!
logging suppress apply rule POST_CERT_EXPIRY
all-of-router
!
```

## Soluzione

- Poiché il router dispone di un altro certificato valido nel pool di trust, l'unico impatto è rappresentato dai messaggi syslog. La scadenza del certificato non influisce sul servizio e i servizi di crittografia possono ancora essere utilizzati.
- È stato aperto l'ID bug Cisco [CSCvs73344](#) che rimuove completamente il certificato dalle versioni XR 7.3.2, 7.3.16, 7.4.1, 7.4.2 e 7.5.1.
- Questo certificato non è più utilizzato da XR, né è un certificato sostitutivo.