

Troubleshoot IOS XR September 30 2021 - DST Root CA X3 Certificate Expiry

Contents

[Introduction](#)

[Sample Certificate](#)

[Pre-September 30 2021](#)

[On and After September 30 2021](#)

[Certificate Expiry Messages](#)

[Workaround](#)

[Pre-Expiry](#)

[Post-Expiry](#)

[Solution](#)

Introduction

This document describes the meaning of the September 30 2021, 'DST Root CA X3' built-in certificate expiration, and any necessary action that is needed to resolve. In most cases, no immediate action is needed.

An external communication from the Root CA publisher is available here:

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

Sample Certificate

```
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

Pre-September 30 2021

Before September 30 2021 users can get a log message that indicates a certificate is about to expire, such as

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

This log message can continue to appear until the certificate expired with a countdown on the number of days.

The 480 days is wrong, the days are mistakenly multiplied by 24 hours, this is handled by Cisco bug ID [CSCvz62603](#).

e.g. $480/24 = 20$ days.

On and After September 30 2021

This certificate is not used and does not cause impact to production traffic or crypto services when the expiry was tested in the lab.

Certificate Expiry Messages

A few different expiry messages can be seen based on your version of code:

```
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.
```

These messages can appear any time the cepki process is restarted or the router is reloaded / Route Processor (RP) is booted.

Workaround

- To disable these syslogs messages, you can configure them to be suppressed, as in this example.
- There is no need to install the replacement certificate, as there is no impact from the certificate expiring.

Pre-Expiry

```
%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-Expiry

```
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
!
```

Solution

- Because the router has another valid certificate in the Trustpool then the only impact is the syslog messages. The certificate expiring is non-service impacting and the crypto services can still be used.
- Cisco bug ID [CSCvs73344](#) has been opened that completely removes this certificate from the XR versions 7.3.2, 7.3.16, 7.4.1, 7.4.2, and 7.5.1.
- This certificate is no longer used by XR, nor is it's replacement certificate.