排除IOS XR 2021年9月30日故障 — DST根CA X3证书到期

目录

简介

本文档介绍2021年9月30日“DST Root CA X3”内置证书过期的含义，以及解决该问题所需的任何必要操作。 在大多数情况下，无需立即采取行动。

从根CA发布方发出的外部通信可在以下位置获得：https://letsencrypt.org/docs/dst-root-ca-x3-expiration-september-2021/

证书示例

```
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
```

2021年9月30日之前

在2021年9月30日之前，用户可以收到指示证书即将过期的日志消息，例如

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

此日志消息可以继续显示，直到证书过期，并在天数中倒计时。

480天错误，天数错误乘以24小时，这由Cisco Bug ID CSCvz62603处理。

例如480/24 = 20天。

2021年9月30日及之后

此证书未使用，在实验室测试到期时不会对生产流量或加密服务造成影响。

证书到期消息

根据您的代码版本，可以看到一些不同的过期消息：

```
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.
```

当cepki进程重新启动或路由器重新加载/路由处理器(RP)启动时，这些消息都会显示。

解决方法

- 要禁用这些系统日志消息，可以将其配置为抑制，如本例所示。
- 无需安装替换证书，因为证书到期不会产生任何影响。

到期前

```
%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
!
```

过期后

```
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
!
```

解决方案

- 由于路由器在Trustpool中有另一个有效证书，因此唯一的影响是系统日志消息。证书即将过期不会影响服务，并且仍然可以使用加密服务。
- 已打开Cisco Bug ID CSCvs73344 ，该ID从XR版本7.3.2、7.3.16、7.4.1、7.4.2和7.5.1中完全删除此证书。
- XR不再使用此证书，也不再使用此证书的替换证书。