IOS XR 2021年9月30日故障排除 — DST根CA X3證書過期

目錄

簡介

本檔案將說明2021年9月30日「DST根CA X3」內建憑證到期的含義，以及需要解決的任何必要動作。 在大多數情況下，不需要立即採取行動。

可以從以下位置獲得來自根CA發佈者的外部通訊：https://letsencrypt.org/docs/dst-root-ca-x3-expiration-september-2021/

證書示例

```
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，使用者可以收到指示證書即將到期的日誌消息，例如

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

此日誌消息可以繼續顯示，直到證書過期，並且倒計時為天數。

480天錯誤，天數被錯誤地乘以24小時，由思科錯誤ID CSCvz62603處理。

例如480/24 = 20天。

2021年9月30日及之後

此證書未使用，並且在實驗室中測試到期時不會對生產流量或加密服務造成影響。

證書到期消息

根據您的代碼版本可以看到一些不同的過期消息：

```
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.
```

只要重新啟動cepki進程或重新啟動路由器/路由處理器(RP)，就會出現這些消息。

因應措施

- 要禁用這些系統日誌消息，可以將它們配置為隱藏，如本例所示。
- 不需要安裝替換證書，因為證書過期不會造成任何影響。

預到期

```
%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
!
```

過期後

```
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
!
```

解決方案

- 由於路由器在Trustpool中有另一個有效證書，因此唯一的影響是系統日誌消息。證書到期不影響服務，並且仍可使用加密服務。
- 已開啟思科錯誤ID CSCvs73344，該漏洞會從XR 7.3.2、7.3.16、7.4.1、7.4.2和7.5.1版中完全刪除此證書。
- XR不再使用此證書，它也不是替代證書。