IOS XR 트러블슈팅 2021년 9월 30일 - DST Root CA X3 인증서 만료

목차

소개

이 문서에서는 2021년 9월 30일, 'DST Root CA X3' 내장 인증서 만기의 의미 및 해결에 필요한 모든 조치를 설명합니다. 대부분의 경우 즉각적인 조치는 필요하지 않습니다.

루트 CA 게시자의 외부 통신은 여기에서 확인할 수 있습니다. https://letsencrypt.org/docs/dst-root-ca-x3-expiration-september-2021/

샘플 인증서

```
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
```

2021년 9월 30일 이전

2021년 9월 30일 이전에 사용자는 인증서가 곧 만료될 예정임을 나타내는 로그 메시지를 받을 수 있습니다.

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

이 로그 메시지는 인증서가 만료될 때까지 계속 표시될 수 있으며, 카운트다운은 일 단위로 진행됩니다.

480일이 잘못되었습니다. 실수로 24시간을 곱한 후 Cisco 버그 ID CSCvz62603으로 처리됩니다.

예: 480/24 = 20일

2021년 9월 30일 이후

이 인증서는 사용되지 않으며 Lab에서 만료가 테스트될 때 프로덕션 트래픽 또는 암호화 서비스에 영향을 미치지 않습니다.

인증서 만료 메시지

사용자의 코드 버전에 따라 몇 가지 만료 메시지를 볼 수 있습니다.

```
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.
```

이러한 메시지는 cepki 프로세스가 다시 시작되거나 라우터가 다시 로드되거나 RP(Route Processor)가 부팅될 때마다 나타날 수 있습니다.

해결 방법

- 이러한 syslogs 메시지를 비활성화하려면 이 예와 같이 억제되도록 구성할 수 있습니다.
- 인증서가 만료되면 영향을 받지 않으므로 교체 인증서를 설치할 필요가 없습니다.

만료 전

```
%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
!
```

만료 후

```
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
!
```

솔루션

- 라우터에 Trustpool에 다른 유효한 인증서가 있으므로 syslog 메시지만 영향을 받습니다. 인증서가 만료될 경우 서비스에 영향을 미치지 않으며 암호화 서비스를 계속 사용할 수 있습니다.

- Cisco 버그 ID CSCvs73344가 열려 XR 버전 7.3.2, 7.3.16, 7.4.1, 7.4.2 및 7.5.1에서 이 인증서를 완전히 제거합니다.
- 이 인증서는 XR에서 더 이상 사용되지 않으며 대체 인증서도 사용하지 않습니다.