IOS XR September 30 2021 - DSTルートCA X3証明書の期限切れのトラブルシューティング

内容

概要

このドキュメントでは、2021年9月30日の「DSTルートCA X3」組み込み証明書の期限切れ、および解決に必要な必要なアクションの意味について説明します。 ほとんどの場合、すぐに行う必要はありません。

ルートCAパブリッシャからの外部通信は、次の場所で利用できます。
https://letsencrypt.org/docs/dst-root-ca-x3-expiration-september-2021/

サンプル証明書

```
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日以前

2021年9月30日より前のバージョンでは、証明書の有効期限が近づいていることを示すログメッセージが表示されます。たとえば、

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

このログメッセージは、証明書がカウントダウン状態で期限切れになるまで表示され続けることができます。

480日が間違っています。日数に誤って24時間を掛けると、これはCisco Bug ID CSCvz62603で処理されます。

例：480/24 = 20日。

2021年9月30日以降

この証明書は使用されず、ラボで期限切れがテストされた場合に実稼働トラフィックや暗号化サービスに影響を与えません。

証明書の期限切れメッセージ

コードのバージョンに基づいて、いくつかの異なる期限切れメッセージが表示されます。

```
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.
```

これらのメッセージは、cepkiプロセスが再起動されるか、ルータがリロードされるか、ルートプロセッサ(RP)がブートされるたびに表示されます。

回避策

- これらのsyslogメッセージを無効にするには、次の例のように、省略するように設定できます。
- 証明書の期限切れによる影響がないため、交換用の証明書をインストールする必要はありません。

期限切れ前

```
%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
!
```

期限切れ後

```
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
!
```

解決方法

- ルータのトラストプールには別の有効な証明書があるため、syslogメッセージが影響を受けるだけです。証明書の期限切れはサービスに影響せず、暗号化サービスを引き続き使用できます。
- Cisco Bug ID CSCvs73344が開かれ、XRバージョン7.3.2、7.3.16、7.4.1、7.4.2、および7.5.1からこの証明書が完全に削除されています。
- この証明書はXRでは使用されなくなり、代替の証明書でもありません。