# Fedora and EPEL updates for various AWS C lib packages

| | |
|---|---|
| **Date:** | 2024-11-25 |
| **modified:** | 2024-11-25 |
| **tags:** | AWS, Fedora, EPEL, Packages, Packaging |
| **description:** | Nine AWS C lib Fedora and EPEL packages I maintain received updates today. |
| **category:** | Linux |
| **slug:** | fedora-and-epel-updates-of-various-aws-c-lib-packages |
| **Author:** | Dominik Wombacher |
| **lang:** | en |
| **transid:** | fedora-and-epel-updates-of-various-aws-c-lib-packages |
| **Status:** | published |

Among the Fedora and EPEL packages I maintain are 11 AWS C lib packages. I wrote some time ago about there function and challenge to package them. Today 9 of those packages received updates to the latest available release. 2 are pending because of dependencies, but I should get them through the door within the next 2-3 weeks as well.

The majority went smoothly, no breaking changes, minor bug fixes, sometimes a patch that had to be updated. But `aws-c-cal` required a bit more work. Whenever tests are available, I run them as part of the package build. And they started to fail when I wanted to update the package:

```
98% tests passed, 3 tests failed out of 137
Total Test time (real) =   3.58 sec
The following tests FAILED:
    66 - rsa_signing_roundtrip_pkcs1_sha1_from_user (Failed)
    71 - rsa_verify_signing_pkcs1_sha1 (Failed)
    77 - rsa_signing_mismatch_pkcs1_sha1 (Failed)
Errors while running CTest
```

The `sha1` in the test name lead me pretty fast to the problem. In version `0.8.1` there was some `SHA1` related code and tests added:

- https://github.com/awslabs/aws-c-cal/releases/tag/v0.8.1
- https://github.com/awslabs/aws-c-cal/pull/201

I can only assume it's for backward compatibility reasons. The thing is, SHA1 is distrusted in Fedora 41 (Archive: [1], [2]) and RHEL 9 (Archive: [1], [2]).

The code provides additional functionality and will not be called on systems that don't use `SHA1` anymore. So the fastest way forward was to patch out the three failing tests and call it a day.

```
diff --git a/tests/CMakeLists.txt b/tests/CMakeLists.txt
index 346e38a..e3966cb 100644
--- a/tests/CMakeLists.txt
+++ b/tests/CMakeLists.txt
@@ -77,18 +77,15 @@ add_test_case(rsa_encryption_roundtrip_oaep_sha256_from_user)
add_test_case(rsa_encryption_roundtrip_oaep_sha512_from_user)
add_test_case(rsa_signing_roundtrip_pkcs1_sha256_from_user)
add_test_case(rsa_signing_roundtrip_pss_sha256_from_user)
-add_test_case(rsa_signing_roundtrip_pkcs1_sha1_from_user)
add_test_case(rsa_getters)
add_test_case(rsa_private_pkcs1_der_parsing)
```

```
add_test_case(rsa_public_pkcs1_der_parsing)
add_test_case(rsa_verify_signing_pkcs1_sha256)
-add_test_case(rsa_verify_signing_pkcs1_sha1)
add_test_case(rsa_verify_signing_pss_sha256)
add_test_case(rsa_decrypt_pkcs1)
add_test_case(rsa_decrypt_oaep256)
add_test_case(rsa_decrypt_oaep512)
add_test_case(rsa_signing_mismatch_pkcs1_sha256)
-add_test_case(rsa_signing_mismatch_pkcs1_sha1)

add_test_case(aes_cbc_NIST_CBCGFSbox256_case_1)
add_test_case(aes_cbc_NIST_CBCVarKey256_case_254)
```

An Overview of all updates today, available in `Rawhide` (F42) latest tomorrow. Around one week till they arrive in all stable Fedora and EPEL branches.

- aws-c-cal, 0.7.4 to 0.8.1
- aws-c-mqtt, 0.10.6 to 0.11.0
- aws-checksums, 0.1.20 to 0.2.2
- aws-c-auth, 0.7.31 to 0.8.0
- s2n-tls, 1.5.3 to 1.5.9
- aws-c-sdkutils 0.1.19 to 0.2.1
- aws-c-event-stream 0.4.3 to 0.5.0
- aws-c-compression 0.2.19 to 0.3.0
- aws-c-common 0.9.28 to 0.10.3

Pending are the updates for aws-c-io and aws-c-http. For `Rawhide` that's a matter of a couple days. Stable Fedora and EPEL branches going to take a bit longer, probably 2-3 weeks.