

Commit c7e8a87

 Browse files

 rjbrown2 committed 2 weeks ago

Merge branch 'advisory-fix-1' of <https://github.com/nasa/CryptoLib-ghsa-q2pc-c3jx-3852> into advisory-fix-1

dev

2 parents af4c39b + ca39cb9 commit c7e8a87

🔍 Filter files...



▼ src/core

 crypto_tc.c

test/unit

 ut_tc_process.c

 **2 files changed** **+60** **-0** lines changed

🔍 Search within code



▼

src/core/crypto_tc.c

+7 00000 ...

```

1871 1871
1872 1872         Crypto_TC_Calc_Lengths(&fecf_len, &segment_hdr_len);
1873 1873
1874 1874 +         if(tc_sdls_processed_frame->tc_header.fl <= TC_FRAME_HEADER_SIZE - segment_hdr_len
1875 1875 +             - fecf_len + 1)
1876 1876 +             {
1877 1877 +                 status = CRYPTO_LIB_ERR_TC_FRAME_LENGTH_UNDERFLOW;
1878 1878 +                 mc_if->mc_log(status);
1879 1879 +                 return status;
1880 1880 +             }
1881 1881
1882 1882 // Parse & Check FECF
1883 1883         Crypto_TC_Parse_Check_FECF(ingest, len_ingest, tc_sdls_processed_frame);

```

[illegible]

```

1293 +     uint8_t *test_frame_pt_b = NULL;
1294 +     int      test_frame_pt_len = 0;
1295 +
1296 +     SecurityAssociation_t *test_association;
1297 +     sa_if->sa_get_from_spi(10, &test_association);
1298 +     test_association->sa_state = SA_OPERATIONAL;
1299 +     test_association->est      = 1;
1300 +     test_association->arsn_len = 0;
1301 +     test_association->shsnf_len = 0;
1302 +
1303 +     crypto_key_t *ekp = NULL;
1304 +     ekp            = key_if->get_key(test_association->ekid);
1305 +     ekp->key_state  = KEY_ACTIVE;
1306 +
1307 +     // Convert input test frame
1308 +     hex_conversion(test_frame_pt_h, (char **)&test_frame_pt_b, &test_frame_pt_len);
1309 +
1310 +     status = Crypto_TC_ProcessSecurity(test_frame_pt_b, &test_frame_pt_len,
1311 +                                       tc_sdls_processed_frame);
1312 +
1313 +     ASSERT_EQ(CRYPTO_LIB_ERR_TC_FRAME_LENGTH_UNDERFLOW, status);
1314 +     free(test_frame_pt_b);
1315 +     free(tc_sdls_processed_frame);
1316 +     Crypto_Shutdown();
1317 + }
1265 1318     UTEST_MAIN();

```

Comments 0



Please [sign in](#) to comment.