Commit ca39cb9

Browse files

Donnie-Ice committed 2 weeks ago

```
TC_process underflow resolved
```

dev 1 parent 45e079a commit ca39cb9

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

```
@@ -1871,6 +1871,13 @@ int32_t Crypto_TC_ProcessSecurity_Cam(uint8_t *ingest, int
*len_ingest, TC_t *tc
1871  1871
1872  1872       Crypto_TC_Calc_Lengths(&fecf_len, &segment_hdr_len);
1873  1873
      1874  +    if(tc_sdls_processed_frame->tc_header.fl <= TC_FRAME_HEADER_SIZE - segment_hdr_len
      - fecf_len + 1)
      1875  +    {
      1876  +        status = CRYPTO_LIB_ERR_TC_FRAME_LENGTH_UNDERFLOW;
      1877  +        mc_if->mc_log(status);
      1878  +        return status;
      1879  +    }
      1880  +
1874  1881       // Parse & Check FECF
1875  1882       Crypto_TC_Parse_Check_FECF(ingest, len_ingest, tc_sdls_processed_frame);
1876  1883
```

test/unit/ut_tc_process.c +53

```
@@ -1262,4 +1262,57 @@ UTEST(TC_PROCESS, TC_KEY_STATE_TEST)
1262 1262     Crypto_Shutdown();
1263 1263 }
1264 1264
1265 + UTEST(TC_PROCESS, TC_HEAP_BUFFER_OVERFLOW_TEST)
1266 + {
1267 +     remove("sa_save_file.bin");
1268 +     // Local Variables
1269 +     int32_t status = CRYPTO_LIB_SUCCESS;
1270 +
1271 +     // Configure Parameters
1272 +     Crypto_Config_CryptoLib(KEY_TYPE_INTERNAL, MC_TYPE_INTERNAL, SA_TYPE_INMEMORY,
          CRYPTOGRAPHY_TYPE_LIBGCRYPT,
1273 +                             IV_INTERNAL, CRYPTO_TC_CREATE_FECF_TRUE,
          TC_PROCESS_SDLS_PDUS_TRUE, TC_HAS_PUS_HDR,
1274 +                             TC_IGNORE_SA_STATE_FALSE, TC_IGNORE_ANTI_REPLAY_TRUE,
          TC_UNIQUE_SA_PER_MAP_ID_FALSE,
1275 +                             TC_CHECK_FECF_TRUE, 0x3F,
          SA_INCREMENT_NONTRANSMITTED_IV_TRUE);
1276 +     // AOS Tests
1277 +     // Crypto_Config_Add_Gvcid_Managed_Parameter(0, 0x0003, 0, TC_HAS_FECF,
          TC_HAS_SEGMENT_HDRS, TC_OCF_NA, 1024,
1278 +     // AOS_FHEC_NA, AOS_IZ_NA, 0);
1279 +     GvcidManagedParameters_t AOS_Managed_Parameters = {
1280 +         0, 0x0003, 0, TC_HAS_FECF, AOS_FHEC_NA, AOS_IZ_NA, 0, TC_HAS_SEGMENT_HDRS,
          1024, TC_OCF_NA, 1};
1281 +     Crypto_Config_Add_Gvcid_Managed_Parameters(AOS_Managed_Parameters);
1282 +
1283 +     status = Crypto_Init();
1284 +
1285 +     TC_t *tc_sdls_processed_frame;
1286 +     tc_sdls_processed_frame = malloc(sizeof(uint8_t) * TC_SIZE);
1287 +     memset(tc_sdls_processed_frame, 0, (sizeof(uint8_t) * TC_SIZE));
1288 +
1289 +     // Test frame setup
1290 +     char    *test_frame_pt_h =
          "080300007f0b000afd020202027fff020202020202020202020202020202029bdd5f3c98dd1c50d27a430"
1291 +
          "a4b6757aa33ec183952a9f76e504eb5f8001066ed6c00c8788e11997f2a058da1633e11fed9851d45"
1292 +
          "7bb31a9637ec8f4f15bc8575a0e7104dba5c666b17f7cccdc2adbff9";
```

```
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,
          tc_sdls_processed_frame);
1311 +
1312 +     ASSERT_EQ(CRYPTO_LIB_ERR_TC_FRAME_LENGTH_UNDERFLOW, status);
1313 +     free(test_frame_pt_b);
1314 +     free(tc_sdls_processed_frame);
1315 +     Crypto_Shutdown();
1316 + }
1317 +
1265 1318   UTEST_MAIN();
```

Comments 0

Please sign in to comment.