OP-TEE / optee_os Public

Code Issues 31 Pull requests 33 Actions Projects Wiki Secu

Commit 16926d5

etienne-lms authored and **jenswi-linaro** committed 16 hours ago

```
ta: pkcs11: check template consistency on get attribute value

Check client template holds consistent attribute area sizes
value on PKCS11_CMD_GET_ATTRIBUTE_SIZE.

Fixes: 783c151 ("ta: pkcs11: Add support for getting object size and attribute value")
Signed-off-by: Etienne Carriere <etienne.carriere@st.com>
Reviewed-by: Jens Wiklander <jens.wiklander@linaro.org>
```

master

1 parent e031c4e commit 16926d5

1 file changed +12 -1

Top

Filter files…

ta/pkcs11/src

object.c

Search within code

ta/pkcs11/src/object.c

```
@@ -840,12 +840,23 @@ enum pkcs11_rc entry_get_attribute_value(struct
pkcs11_client *client,
840 840         for (; cur < end; cur += len) {
841 841             struct pkcs11_attribute_head *cli_ref = (void *)cur;
842 842             struct pkcs11_attribute_head cli_head = { };
    843 +           uintptr_t cli_end = 0;
843 844             void *data_ptr = NULL;
844 845
```

```
        846 +          if ((char *)(cli_ref + 1) > end) {
        847 +              rc = PKCS11_CKR_ARGUMENTS_BAD;
        848 +              goto out;
        849 +          }
        850 +
845     851            /* Make copy of header so that is aligned properly. */
846     852            TEE_MemMove(&cli_head, cli_ref, sizeof(cli_head));
847     853
848             -      len = sizeof(*cli_ref) + cli_head.size;
        854 +      if (ADD_OVERFLOW(sizeof(*cli_ref), cli_head.size, &len) ||
        855 +          ADD_OVERFLOW((uintptr_t)cur, len, &cli_end) ||
        856 +          (char *)cli_end > end) {
        857 +          rc = PKCS11_CKR_ARGUMENTS_BAD;
        858 +          goto out;
        859 +      }
849     860
850     861            /* Treat hidden attributes as missing attributes */
851     862            if (attribute_is_hidden(&cli_head)) {
```

Comments 0

Please sign in to comment.