OP-TEE / optee_os Public

Code Issues 31 Pull requests 33 Actions Projects Wiki Secu

Commit e031c4e

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

```
ta: pkcs11: check output buffer size on get attribute value

Check client output buffer input size and update its output
size on PKCS11_CMD_GET_ATTRIBUTE_VALUE command.

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 496fea3 commit e031c4e

1 file changed +10

Top

Filter files…

ta/pkcs11/src

object.c

Search within code

ta/pkcs11/src/object.c

```
@@ -800,6 +800,15 @@ enum pkcs11_rc entry_get_attribute_value(struct
pkcs11_client *client,
800 800             goto out;
801 801         }
802 802
    803 +     /*
    804 +      * We will update the template with relevant data, without resizing it.
    805 +      * Upon completion, it will be copied to client output buffer.
```

```
                806 +       */
                807 +      if (out->memref.size < sizeof(*template) + template->attrs_size) {
                808 +          rc = PKCS11_CKR_ARGUMENTS_BAD;
                809 +          goto out;
                810 +      }
                811 +
803             812         /* Iterate over attributes and set their values */
804             813         /*
805             814          * 1. If the specified attribute (i.e., the attribute specified by the
                    @@ -912,6 +921,7 @@ enum pkcs11_rc entry_get_attribute_value(struct
                    pkcs11_client *client,
912             921             rc = PKCS11_CKR_BUFFER_TOO_SMALL;
913             922
914             923         /* Move updated template to out buffer */
                924 +       out->memref.size = sizeof(*template) + template->attrs_size;
915             925         TEE_MemMove(out->memref.buffer, template, out->memref.size);
916             926
917             927         DMSG("PKCS11 session %"PRIu32": get attributes %#"PRIx32,
```

Comments 0

Please sign in to comment.