strongSwan - Issue #2493

Pkcs11 Plugin Returns w/Bogus Return Code

12.12.2017 10:41 - Jordan Hrycaj

Status:	Feedback		
Priority:	Normal		
Assignee:	Jordan Hrycaj		
Category:	libstrongswan		
Affected version:	5.5.3	**Resolution:**	

Description

The pkcs#11 function C_WaitForSlotEvent() may return CKR_FUNCTION_FAILED and not initialise a
slot_id (see pkcs#11 doc, chapter 11.5, p110f). In that case the plugin (see pkcs11_manager.c(191)) will log an error
but still use the uninitialised slot_id nevertheless.

I added a little patch to fix that (applies to 5.5.3++).

History

#1 - 12.12.2017 11:12 - Tobias Brunner

- Status changed from New to Feedback

> The pkcs#11 function C_WaitForSlotEvent() may return CKR_FUNCTION_FAILED and not initialise a
> slot_id (see pkcs#11 doc, chapter 11.5, p110f). In that case the plugin (see pkcs11_manager.c(191)) will log an error
> but still use the uninitialised slot_id nevertheless.

While I see that CKR_FUNCTION_FAILED is listed as possible return value (with a bunch of other generic errors) PKCS#11 does not describe any possible reasons for it. When exactly does this occur? Depending on that (e.g. if it occasionally occurs due to some temporary failure) it might be better to actually retry calling C_WaitForSlotEvent(), that is, return e.g. JOB_REQUEUE_FAIR.

#2 - 12.12.2017 15:33 - Jordan Hrycaj

It occurs within a pkcs#11 lib when it decides that it has no wait discipline available, for instance.

The problem is the expectation of a variable to be initialised although the return value is not OK.

BTW, the first paragraph p110 states, that "pSlot points to a location which will receive the ID of the
slot that the event occurred in." So there is no reason to expect initialisation unless an event occurs
(open for interpretation though defensive programming would assume the worst, anyway.)

#3 - 12.12.2017 15:58 - Tobias Brunner

> It occurs within a pkcs#11 lib when it decides that it has no wait discipline available, for instance.

What's a "wait discipline" and how could it not be available?

> The problem is the expectation of a variable to be initialised although the return value is not OK.

Yes, obviously, but since this never happened so far (there also have never been reports of a library returning this error code) I'm wondering when and why that's the case and if it's a fatal issue (return JOB_REQUEUE_NONE and disable slot events) or an intermittent occurrence (return JOB_REQUEUE_FAIR or JOB_RESCHEDULE and retry again).

Files

0002-BUGFIX-handle-all-return-codes-from-pkcs-11-library-.patch	848 Bytes	12.12.2017	Jordan Hrycaj