

strongSwan - Bug #165

ASN1 parser date overflows

20.12.2011 10:08 - Erick Turnquist

Status:	Closed	Start date:	20.12.2011
Priority:	Normal	Due date:	
Assignee:	Tobias Brunner	Estimated time:	0.00 hour
Category:	libstrongswan	Resolution:	
Target version:	4.6.2		
Affected version:	4.6.1		

Description

I have discovered some C casting errors that cause extremely large ASN1 dates to overflow and go undetected. Attached to this issue is a patch to correct the errors I found. This will turn this incorrect expiration date:

not after Sep 02 01:04:44 1975, expired (13258 days ago)

into

not after Oct 09 07:33:00 2111, ok

History

#1 - 23.12.2011 16:46 - Tobias Brunner

- Category set to libstrongswan
- Status changed from New to Resolved
- Assignee set to Tobias Brunner
- Target version set to 4.6.2

Hi Erick,

Thanks for the report. Fixed in master.

Regards,
Tobias

#2 - 30.01.2012 11:10 - Tobias Brunner

- Status changed from Resolved to Closed

Files

asn1-date-overflow.patch

870 Bytes

20.12.2011

Erick Turnquist