Anubis - Bug #47
Displaying a SSL certificate make the VM to crash

07/18/2008 05:00 PM - Anonymous

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Alain Prouté	**% Done:**	0%
Category:	Virtual Machine	**Estimated time:**	0.00 hour
Target version:	1.10		
Platform:		**Triage Stage:**	
Resolution:			

Description

Using the function to_string(X509) can crash the VM (at least on Windows), depending of the content of the certificate.

History

#1 - 07/19/2008 01:21 PM - Alain Prouté

This problem is known since the beginning. Probably a bug in SSL. Cannot do much except encapsulate the SSL call into a 'sigsegv_protect' (macro defined in vm.h). Actually I see that it is already the case, so that I don't understand what you mean by 'crash'.

#2 - 07/19/2008 01:40 PM - Alain Prouté

Is SIGSEGV actually trapped under Windows ?

#3 - 07/21/2008 02:36 PM - Anonymous

I don't really known ifSIGSEGV is trapped or no under Windows (I think no...), but I'm confident this is not a great maner to check if the certificate is well formed or no. I think we should avoid completely the use of such exceptions that can have very big side effects.

Even more, the error can be masked because the exception doesn't occure (write into allowed memory block, but not into the rigth struct... results are uncertains).

#4 - 07/21/2008 02:42 PM - Alain Prouté

The problem is that when we call a third party library function we cannot trust this library. This is why Apache for example encapsulates library calls (and plug-ins calls) into a mecanism using setjmp and longjump and trapping exceptions. I did the same with the macro 'sigsegv_protect'. If we want something better we need to replace the library function by a functoin of our own, either in C or in Anubis.

As far as the printing of X509 certificates is concerned, I thing reasonable to try to do it in Anubis. It should not be too complicated.

#5 - 01/20/2009 09:00 AM - Anonymous

- Target version changed from 1.9 to 1.10

- Platform deleted (Windows)

- 3 deleted (Not started)