Anubis - Bug #60
Assertion into VM 1.10.0.0

01/29/2009 11:34 PM - Anonymous

Status:	Resolved	**Start date:**	01/29/2009
Priority:	Immediate	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Virtual Machine	**Estimated time:**	0.00 hour
Target version:	1.10		
Platform:	All	**Triage Stage:**	
Resolution:			

Description

Upgrading VM from version 1.9.1.12 to version 1.10.0.0, one of our application doesn't start any more. The Anubis VM close itself with following message :

```
anbexec: /home/ricard/develop/anubis/anubis_dev/vm/src/serialize.cpp:1391: static void
CM::AnubisProcess::ui_indirect_type_Int(CM::AnubisProcess*): Assertion `nb != 0' failed.
Aborted
```

As this application contains a Web Server which use serialized states on disk, it should be the unserializing of a state which fails.

History

#1 - 01/30/2009 12:31 AM - Alain Prouté

- Assignee changed from Alain Prouté to Anonymous

Cédric RICARD wrote:

> *Upgrading VM from version 1.9.1.12 to version 1.10.0.0, one of our application doesn't start any more. The Anubis VM close itself with following message :*
> *[...]*
>
> *As this application contains a Web Server which use serialized states on disk, it should be the unserializing of a state which fails.*

This is actually a bug in serialize.cpp. The case nb 0 (nb number of bigits) line 1391 must be treated in the same way as the case (nb > 0x3fffffe || (4*(nb+1)) > (U32)(free_sdata)) just above. If one of these tests fails, the datum cannot be unserialized. In this situation, one must set the flag:

ufflag = 1;

and:

(1) in the case of an indirect unserialization instruction, do the following:

```
((MAM(m_SP)-1))) = 0;    /* put the fake datum '0' instead of the unserialized datum /
    *(MAM(m_SP)-1) += 4;          / position the destination pointer one word higher for the next datum */
```

(2) in the case of a direct unserialization instruction, do the following:

```
MAM(m_R) = 0;                /* put the fake datum '0' in R */
```

We have exactly the same bug at line 1305 (type_Int).

Notice: 'ui_decl' = unserialization instruction'
'si_decl' = serialization instruction

I did not modify the source. I let Cédric perform the correction.

#2 - 02/14/2009 07:24 PM - Alain Prouté

- Status changed from New to Resolved

Fixed.