Subject: Crash in tt.dll
Posted by Xpert on Wed, 25 Jul 2012 02:56:11 GMT
View Forum Message <> Reply to Message

My first server side crash in over a month.
It points to tt.dll

File Attachments

1) ax-crash.rar, downloaded 219 times

Subject: Re: Crash in tt.dll
Posted by StealthEye on Mon, 30 Jul 2012 14:28:19 GMT
View Forum Message <> Reply to Message

This is very weird, it ended up calling a dtor for an object while still running its ctor. Unless you hook Set_Object_Dirty_Bits in some plugin or something, I can't see how this happened.

Subject: Re: Crash in tt.dll
Posted by danpaul88 on Mon, 30 Jul 2012 15:01:58 GMT
View Forum Message <> Reply to Message

StealthEye wrote on Mon, 30 July 2012 15:28This is very weird, it ended up calling a dtor for an object while still running its ctor. Unless you hook Set_Object_Dirty_Bits in some plugin or something, I can't see how this happened.

```
class Object
{
  Object::Object
  {
    delete this;
  }

  Object::~Object
  {
    printf ( "BOOM!");
  }
}
```

Subject: Re: Crash in tt.dll
Posted by StealthEye on Mon, 30 Jul 2012 16:56:10 GMT
View Forum Message <> Reply to Message

Exactly, but then without the "delete this" call. It seems to have jumped right from the ctor to the dtor for no apparent reason/cause.

Subject: Re: Crash in tt.dll
Posted by danpaul88 on Mon, 30 Jul 2012 17:50:42 GMT
View Forum Message <> Reply to Message

Could be stack corruption possibly? Does the call stack higher up look sensible for constructing the object in question in the first place?

Subject: Re: Crash in tt.dll
Posted by Xpert on Mon, 30 Jul 2012 21:57:37 GMT
View Forum Message <> Reply to Message

StealthEye wrote on Mon, 30 July 2012 10:28This is very weird, it ended up calling a dtor for an object while still running its ctor. Unless you hook Set_Object_Dirty_Bits in some plugin or something, I can't see how this happened.

I never used that in any of my code. I wouldn't know how to use Set_Object_Dirty_Bits lol

---

Subject: Re: Crash in tt.dll
Posted by StealthEye on Tue, 31 Jul 2012 14:52:03 GMT
View Forum Message <> Reply to Message

danpaul88, it looks sensible for constructing the object, not for destructing it. I can't think of why it would destroy the object, but it would be strange if the dtor appeared on the stack at that point coincidentally too. My guess is that somehow the vtable (or pointer to vtable) was messed up, and it called the dtor instead of Set_Object_Dirty_Bits. This is still quite unlikely though.
