
Subject: Server crash dump

Posted by [Lazy5686](#) on Fri, 31 May 2013 20:49:32 GMT

[View Forum Message](#) <> [Reply to Message](#)

First one in a while.

EDIT: Iran pointed out that the size is 0 kB, just checked the original and it says it is 0 bytes.

File Attachments

1) [crashdump_May_31_2013.zip](#), downloaded 243 times

Subject: Re: Server crash dump

Posted by [danpaul88](#) on Sat, 01 Jun 2013 20:03:48 GMT

[View Forum Message](#) <> [Reply to Message](#)

That happens sometimes, I think the crashdump code fails to initialise properly with certain types of crash so it's unable to output the file completely.

Subject: Re: Server crash dump

Posted by [saberhawk](#) on Sat, 01 Jun 2013 20:24:29 GMT

[View Forum Message](#) <> [Reply to Message](#)

danpaul88 wrote on Sat, 01 June 2013 13:03 That happens sometimes, I think the crashdump code fails to initialise properly with certain types of crash so it's unable to output the file completely.

Indeed, it's very difficult to write code that works correctly in a crashing process because, by definition, the process is in a very bad state where things don't work completely right anymore.

Subject: Re: Server crash dump

Posted by [Lazy5686](#) on Sat, 01 Jun 2013 22:37:13 GMT

[View Forum Message](#) <> [Reply to Message](#)

It did the same thing again today, crash dump is 0 bytes.

We were playing Under, Nod was rushing with a bunch of tanks. Connection lost.

Go into the FDS console and it said it had lost connection with XWIS, although none of our other servers running at that time had crashed.

Subject: Re: Server crash dump

Posted by [Ethenal](#) on Sat, 01 Jun 2013 23:51:04 GMT

[View Forum Message](#) <> [Reply to Message](#)

I imagine it is quite related to the fact we just updated our scripts to r5276, also with raven's additions, which could certainly be the cause of these crashes but I won't say that for sure.

We haven't had many crashes lately aside from the weird score overflow thing right?

Subject: Re: Server crash dump
Posted by [crushu06](#) on Sun, 02 Jun 2013 05:27:23 GMT
[View Forum Message](#) <> [Reply to Message](#)

Ethenal wrote on Sat, 01 June 2013 16:51 with raven's additions

Yup nuff said

Subject: Re: Server crash dump
Posted by [BAGUETTE](#) on Sun, 02 Jun 2013 14:24:07 GMT
[View Forum Message](#) <> [Reply to Message](#)

why does raven get blamed for everything lmao

Subject: Re: Server crash dump
Posted by [ehhh](#) on Sun, 02 Jun 2013 14:40:21 GMT
[View Forum Message](#) <> [Reply to Message](#)

I'd love some raven additions

Subject: Re: Server crash dump
Posted by [StealthEye](#) on Sun, 02 Jun 2013 15:05:21 GMT
[View Forum Message](#) <> [Reply to Message](#)

Possibly this is due to a known (now fixed) memory leak (a crashdump ending up empty may well be caused by that). Can you keep an eye on the memory usage in case it crashes again?

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Sun, 02 Jun 2013 23:12:08 GMT
[View Forum Message](#) <> [Reply to Message](#)

StealthEye wrote on Sun, 02 June 2013 08:05Possibly this is due to a known (now fixed) memory leak (a crashdump ending up empty may well be caused by that). Can you keep an eye on the memory usage in case it crashes again?

Just had another crash but I had not seen this post, I've sent you a pm but we will keep an eye on the memory usage.

Although we just patched a leak caused by one of our plugins a few days ago, Raven update our scripts to release 5276 so that could be causing issues.

Subject: Re: Server crash dump
Posted by [Ethenal](#) on Wed, 05 Jun 2013 16:09:28 GMT
[View Forum Message](#) <> [Reply to Message](#)

I'm not blaming raven, but our scripts.dll is indeed modified so we could have very well screwed up ourselves however, I have yet to see a 0byte crashdump until now...

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Wed, 05 Jun 2013 18:22:12 GMT
[View Forum Message](#) <> [Reply to Message](#)

One finally generated with data in it.

File Attachments

1) [crashdump.20130605-181150-r5276-n1.dmp](#), downloaded 252 times

Subject: Re: Server crash dump
Posted by [StealthEye](#) on Wed, 05 Jun 2013 21:14:57 GMT
[View Forum Message](#) <> [Reply to Message](#)

It crashes in taunts.dll, so whoever has the matching taunts.pdb file should debug it.

Subject: Re: Server crash dump
Posted by [Xpert](#) on Thu, 06 Jun 2013 08:21:53 GMT
[View Forum Message](#) <> [Reply to Message](#)

StealthEye wrote on Wed, 05 June 2013 17:14 It crashes in taunts.dll, so whoever has the matching taunts.pdb file should debug it.

Iran!

Subject: Re: Server crash dump
Posted by [iRANian](#) on Thu, 06 Jun 2013 18:03:52 GMT

Crashed in MDB_SSGM_KeyHook_Clone::Destroyed(GameObject *obj) while Calling ::RemoveHook, which I added to the plugin by copying it from the SSGM 2.0.2 source:

```
void MDB_SSGM_KeyHook_Clone::Destroyed(GameObject *obj) {  
    if (is_keyhook_set == 1337) {  
        RemoveHook();  
    }  
}
```

```
void MDB_SSGM_KeyHook_Clone::RemoveHook() {  
    if (hookid != 0 && RemoveKeyHook != 0) {  
        RemoveKeyHook(hookid);  
        hookid = 0;  
        if (k != 0) {  
            delete[] k->key;  
            delete k;  
            k = 0;  
        }  
    }  
}
```

```
70: void MDB_SSGM_KeyHook_Clone::Destroyed(GameObject *obj) {  
730F12A0 56          push     esi  
730F12A1 8B F1      mov     esi,ecx  
71: if (is_keyhook_set == 1337) {  
730F12A3 81 7E 24 39 05 00 00 cmp     dword ptr [esi+24h],539h  
730F12AA 75 45      jne     MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)  
72: RemoveHook();  
730F12AC 8B 46 20      mov     eax,dword ptr [esi+20h]  
730F12AF 85 C0      test    eax,eax  
730F12B1 74 3E      je      MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)  
730F12B3 8B 0D F0 20 0F 73 mov     ecx,dword ptr [__imp_RemoveKeyHook (730F20F0h)]  
730F12B9 8B 09      mov     ecx,dword ptr [ecx]  
730F12BB 85 C9      test    ecx,ecx  
730F12BD 74 32      je      MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)  
730F12BF 50          push    eax  
730F12C0 FF D1      call    ecx  
730F12C2 8B 46 1C      mov     eax,dword ptr [esi+1Ch]  
730F12C5 83 C4 04      add     esp,4  
730F12C8 C7 46 20 00 00 00 00 mov     dword ptr [esi+20h],0  
730F12CF 85 C0      test    eax,eax  
730F12D1 74 1E      je      MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)  
730F12D3 8B 50 04      mov     edx,dword ptr [eax+4] // CRASHES HERE  
730F12D6 52          push    edx  
730F12D7 FF 15 80 20 0F 73 call    dword ptr [__imp_operator delete[] (730F2080h)]  
730F12DD 8B 46 1C      mov     eax,dword ptr [esi+1Ch]  
730F12E0 50          push    eax
```

```
730F12E1 FF 15 88 20 0F 73  call    dword ptr [__imp_operator delete (730F2088h)]
730F12E7 83 C4 08          add     esp,8
730F12EA C7 46 1C 00 00 00 00 mov     dword ptr [esi+1Ch],0
730F12F1 5E                pop     esi
73: }
74: }
```

Registers:

```
EDX 730F22F0
EAX 0000001F
EBP 0018FAF0
AL 1F
```

The value of the 'k' pointer variable (which is of type KeyHookStruct)somehow was set to 0x1F instead of a valid pointer address, then the code tries to access memory address variable 'k' + 4 (0x1f + 4) which is invalid and the server crashed.

Subject: Re: Server crash dump
Posted by [StealthEye](#) on Thu, 06 Jun 2013 20:11:07 GMT
[View Forum Message](#) <> [Reply to Message](#)

I don't think any of those functions are wrong. Perhaps the actual issue is in a function up stack?
Or memory corruption surrounding that location?

Subject: Re: Server crash dump
Posted by [raven](#) on Thu, 06 Jun 2013 20:39:38 GMT
[View Forum Message](#) <> [Reply to Message](#)

when in doubt, blame me

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Fri, 07 Jun 2013 02:25:23 GMT
[View Forum Message](#) <> [Reply to Message](#)

raven wrote on Thu, 06 June 2013 13:39

when in doubt, blame me
If it makes you feel any better I disabled a couple of Iran's plugins.

At the very least, we haven't seen the SFPS drops we used to.

Subject: Re: Server crash dump
Posted by [iRANian](#) on Fri, 07 Jun 2013 07:48:16 GMT
[View Forum Message](#) <> [Reply to Message](#)

So SFPS drops are fixed now?

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Fri, 07 Jun 2013 13:07:50 GMT
[View Forum Message](#) <> [Reply to Message](#)

iRANian wrote on Fri, 07 June 2013 00:48: So SFPS drops are fixed now?
Looks like it.

Subject: Re: Server crash dump
Posted by [iRANian](#) on Fri, 07 Jun 2013 19:55:08 GMT
[View Forum Message](#) <> [Reply to Message](#)

How do you know? You disabled it yesterday and the server just got restarted now.

Subject: Re: Server crash dump
Posted by [raven](#) on Fri, 07 Jun 2013 23:56:12 GMT
[View Forum Message](#) <> [Reply to Message](#)

Wouldn't that be funny? Iran complaining that my scripts were causing SFPS drops, yet it turns out to be his.

Subject: Re: Server crash dump
Posted by [Gen_Blacky](#) on Sat, 08 Jun 2013 00:53:30 GMT
[View Forum Message](#) <> [Reply to Message](#)

raven wrote on Fri, 07 June 2013 17:56: Wouldn't that be funny? Iran complaining that my scripts were causing SFPS drops, yet it turns out to be his.

Either case its still Ravens fault!

Subject: Re: Server crash dump
Posted by [Xpert](#) on Sat, 08 Jun 2013 02:04:52 GMT
[View Forum Message](#) <> [Reply to Message](#)

raven wrote on Fri, 07 June 2013 19:56Wouldn't that be funny? Iran complaining that my scripts were causing SFPS drops, yet it turns out to be his.

Iran purposely sabotaged Jelly. I KNEW IT. God damn it raven.

Subject: Re: Server crash dump
Posted by [iRANian](#) on Sat, 08 Jun 2013 10:27:59 GMT
[View Forum Message](#) <> [Reply to Message](#)

and i would have gotten away with it if it werent for you meddling kids

Subject: Re: Server crash dump
Posted by [Jerad2142](#) on Sat, 08 Jun 2013 19:52:12 GMT
[View Forum Message](#) <> [Reply to Message](#)

iRANian wrote on Thu, 06 June 2013 12:03Crashed in
MDB_SSGM_KeyHook_Clone::Destroyed(GameObject *obj) while Calling ::RemoveHook, which I added to the plugin by copying it from the SSGM 2.0.2 source:

```
void MDB_SSGM_KeyHook_Clone::Destroyed(GameObject *obj) {  
    if (is_keyhook_set == 1337) {  
        RemoveHook();  
    }  
}
```

```
void MDB_SSGM_KeyHook_Clone::RemoveHook() {  
    if (hookid != 0 && RemoveKeyHook != 0) {  
        RemoveKeyHook(hookid);  
        hookid = 0;  
        if (k != 0) {  
            delete[] k->key;  
            delete k;  
            k = 0;  
        }  
    }  
}
```

```
70: void MDB_SSGM_KeyHook_Clone::Destroyed(GameObject *obj) {  
730F12A0 56          push     esi  
730F12A1 8B F1        mov     esi,ecx
```

```

71: if (is_keyhook_set == 1337) {
730F12A3 81 7E 24 39 05 00 00 cmp     dword ptr [esi+24h],539h
730F12AA 75 45                jne     MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)
72: RemoveHook();
730F12AC 8B 46 20                mov     eax,dword ptr [esi+20h]
730F12AF 85 C0                test    eax,eax
730F12B1 74 3E                je      MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)
730F12B3 8B 0D F0 20 0F 73      mov     ecx,dword ptr [__imp_RemoveKeyHook (730F20F0h)]
730F12B9 8B 09                mov     ecx,dword ptr [ecx]
730F12BB 85 C9                test    ecx,ecx
730F12BD 74 32                je      MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)
730F12BF 50                push    eax
730F12C0 FF D1                call    ecx
730F12C2 8B 46 1C                mov     eax,dword ptr [esi+1Ch]
730F12C5 83 C4 04                add     esp,4
730F12C8 C7 46 20 00 00 00 00 mov     dword ptr [esi+20h],0
730F12CF 85 C0                test    eax,eax
730F12D1 74 1E                je      MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)
730F12D3 8B 50 04                mov     edx,dword ptr [eax+4] // CRASHES HERE
730F12D6 52                push    edx
730F12D7 FF 15 80 20 0F 73      call    dword ptr [__imp_operator delete[] (730F2080h)]
730F12DD 8B 46 1C                mov     eax,dword ptr [esi+1Ch]
730F12E0 50                push    eax
730F12E1 FF 15 88 20 0F 73      call    dword ptr [__imp_operator delete (730F2088h)]
730F12E7 83 C4 08                add     esp,8
730F12EA C7 46 1C 00 00 00 00 mov     dword ptr [esi+1Ch],0
730F12F1 5E                pop     esi
73: }
74: }

```

Registers:

```

EDX 730F22F0
EAX 0000001F
EBP 0018FAF0
AL 1F

```

The value of the 'k' pointer variable (which is of type KeyHookStruct)somehow was set to 0x1F instead of a valid pointer address, then the code tries to access memory address variable 'k' + 4 (0x1f + 4) which is invalid and the server crashed.

Perhaps it was destroyed before the create function was completed thus k was not yet set to 0. Easiest way to protect against this is to attach a dummy script when the create function is done. Then check to see if this dummy script is attached before doing any point related operations on delete, custom, or damaged events (or anything other events that could potentially get called before create is done).

Subject: Re: Server crash dump
Posted by [iRANian](#) on Sat, 08 Jun 2013 20:34:57 GMT
[View Forum Message](#) <> [Reply to Message](#)

That code is from SSGM 2.0.2.

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Sun, 09 Jun 2013 01:28:39 GMT
[View Forum Message](#) <> [Reply to Message](#)

Well it went one day without crashing.

Back to disabling a few more plugins at a time before we find the culprit.

Subject: Re: Server crash dump
Posted by [Jerad2142](#) on Sun, 09 Jun 2013 17:41:19 GMT
[View Forum Message](#) <> [Reply to Message](#)

iRANian wrote on Sat, 08 June 2013 14:34 That code is from SSGM 2.0.2.
Ah, then I have 0 ideas.

Subject: Re: Server crash dump
Posted by [iRANian](#) on Sun, 09 Jun 2013 20:34:23 GMT
[View Forum Message](#) <> [Reply to Message](#)

It was running on the server for about 9 months or so, this crash happened after an update to the latest 4.0 server code, but I'm not sure if it's related. It's very weird though..

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Tue, 18 Jun 2013 19:02:42 GMT
[View Forum Message](#) <> [Reply to Message](#)

Here's another.

<http://jelly-server.com/crashdump.20130618-185021-r5276-n1.dmp>

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Wed, 19 Jun 2013 15:10:31 GMT
[View Forum Message](#) <> [Reply to Message](#)

No edit button?

Anyways, happened a minute after Mesa loaded.
<http://jelly-server.com/crashdump.20130619-150302-r5276-n1.dmp>

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Wed, 19 Jun 2013 19:56:52 GMT
[View Forum Message](#) <> [Reply to Message](#)

<http://jelly-server.com/crashdump.20130619-194903-r5276-n1.dmp>

Subject: Re: Server crash dump
Posted by [Gen_Blacky](#) on Wed, 19 Jun 2013 21:55:50 GMT
[View Forum Message](#) <> [Reply to Message](#)

Its Ravens fault!

Subject: Re: Server crash dump
Posted by [EvilWhiteDragon](#) on Wed, 19 Jun 2013 23:37:09 GMT
[View Forum Message](#) <> [Reply to Message](#)

I do wonder why this only seems to happen on Jelly, and only seems to have started recently while no new build was released.

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Thu, 20 Jun 2013 02:11:29 GMT
[View Forum Message](#) <> [Reply to Message](#)

EvilWhiteDragon wrote on Wed, 19 June 2013 16:37 I do wonder why this only seems to happen on Jelly, and only seems to have started recently while no new build was released.
We just updated from the previous build a few weeks ago.

Subject: Re: Server crash dump
Posted by [Ethenal](#) on Thu, 20 Jun 2013 06:21:11 GMT
[View Forum Message](#) <> [Reply to Message](#)

Lazy5686 wrote on Wed, 19 June 2013 21:11 EvilWhiteDragon wrote on Wed, 19 June 2013 16:37 I do wonder why this only seems to happen on Jelly, and only seems to have started recently while no new build was released.
We just updated from the previous build a few weeks ago.

Yeah haha, we were a bit behind the times. We haven't been on the new version until like, the past week I think.

Subject: Re: Server crash dump
Posted by [iRANian](#) on Thu, 20 Jun 2013 07:22:03 GMT
[View Forum Message](#) <> [Reply to Message](#)

Is the server running matching scripts.dll and tt.dll versions yet?

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Tue, 25 Jun 2013 01:37:29 GMT
[View Forum Message](#) <> [Reply to Message](#)

iRANian wrote on Thu, 20 June 2013 00:22: Is the server running matching scripts.dll and tt.dll versions yet?
We are now.

If only XWIS could come back online...

Subject: Re: Server crash dump
Posted by [EvilWhiteDragon](#) on Tue, 25 Jun 2013 08:45:30 GMT
[View Forum Message](#) <> [Reply to Message](#)

Ehmm, why were you mix&matching different versions of scripts.dll and TT.dll AND complaining about crashes?

Subject: Re: Server crash dump
Posted by [Ethenal](#) on Tue, 25 Jun 2013 14:58:45 GMT
[View Forum Message](#) <> [Reply to Message](#)

Well it was an accident, obviously

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Tue, 25 Jun 2013 19:41:30 GMT
[View Forum Message](#) <> [Reply to Message](#)

EvilWhiteDragon wrote on Tue, 25 June 2013 01:45: Ehmm, why were you mix&matching different versions of scripts.dll and TT.dll AND complaining about crashes?
We thought raven had been using the same versions of everything. He hasn't sent anyone his source yet so I don't even know what the differences were.

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Wed, 26 Jun 2013 17:07:43 GMT
[View Forum Message](#) <> [Reply to Message](#)

Running stock scripts.dll, scripts2.dll and tt.dll. All the latest version.

<http://jelly-server.com/crashdump.20130626-163732-r5276-n1.dmp>

EDIT:

[14:06:48] <iran> crashes inside tt.dll
[14:09:13] <iran> call stack might be corrupted
[14:10:56] <iran> ask them where it crashed

Subject: Re: Server crash dump
Posted by [iRANian](#) on Wed, 26 Jun 2013 17:23:47 GMT
[View Forum Message](#) <> [Reply to Message](#)

I checked a few of the other crashdumps in this thread and except the one crashing inside taunts.dll the other ones crash at the same point:

70AC3B42 FF 46 58 inc dword ptr [esi+58h]

Could this be a plugin or something that's causing the crash?

Subject: Re: Server crash dump
Posted by [raven](#) on Mon, 01 Jul 2013 01:00:48 GMT
[View Forum Message](#) <> [Reply to Message](#)

Lazy5686 wrote on Tue, 25 June 2013 12:41 EvilWhiteDragon wrote on Tue, 25 June 2013 01:45 Ehmm, why were you mix&matching different versions of scripts.dll and TT.dll AND complaining about crashes?

We thought raven had been using the same versions of everything. He hasn't sent anyone his source yet so I don't even know what the differences were.

The source is posted on git...

Subject: Re: Server crash dump
Posted by [Lazy5686](#) on Mon, 01 Jul 2013 02:44:25 GMT
[View Forum Message](#) <> [Reply to Message](#)

raven wrote on Sun, 30 June 2013 18:00 Lazy5686 wrote on Tue, 25 June 2013 12:41 EvilWhiteDragon wrote on Tue, 25 June 2013 01:45 Ehmm, why were you mix&matching

different versions of scripts.dll and TT.dll AND complaining about crashes?

We thought raven had been using the same versions of everything. He hasn't sent anyone his source yet so I don't even know what the differences were.

The source is posted on git...

Well we're running something different right now as Iran and Stealtheye fixed the cause of the crashes that were plaguing us the last few weeks.

Subject: Re: Server crash dump

Posted by [iRANian](#) on Mon, 01 Jul 2013 07:07:04 GMT

[View Forum Message](#) <> [Reply to Message](#)

StealthEye fixed them, not me.

Subject: Re: Server crash dump

Posted by [Ethenal](#) on Mon, 01 Jul 2013 14:39:56 GMT

[View Forum Message](#) <> [Reply to Message](#)

raven wrote on Sun, 30 June 2013 20:00Lazy5686 wrote on Tue, 25 June 2013

12:41EvilWhiteDragon wrote on Tue, 25 June 2013 01:45Ehmm, why were you mix&matching different versions of scripts.dll and TT.dll AND complaining about crashes?

We thought raven had been using the same versions of everything. He hasn't sent anyone his source yet so I don't even know what the differences were.

The source is posted on git...oh now you listen to me

Subject: Re: Server crash dump

Posted by [Xpert](#) on Mon, 01 Jul 2013 16:40:11 GMT

[View Forum Message](#) <> [Reply to Message](#)

Ethenal wrote on Mon, 01 July 2013 10:39raven wrote on Sun, 30 June 2013 20:00Lazy5686

wrote on Tue, 25 June 2013 12:41EvilWhiteDragon wrote on Tue, 25 June 2013 01:45Ehmm, why were you mix&matching different versions of scripts.dll and TT.dll AND complaining about crashes?

We thought raven had been using the same versions of everything. He hasn't sent anyone his source yet so I don't even know what the differences were.

The source is posted on git...oh now you listen to me

I bugged him yesterday on IRC for it lol.
