Subject: 3.4.4 Send_Message_Player Disconnect
Posted by Jerad2142 on Sat, 06 Feb 2010 19:17:30 GMT
View Forum Message <> Reply to Message

In scripts 3.4.4, if you send a string of more than 238 chars it will cause the receiving client to lose their connection (Or possibly all clients, this has only been tested during 2v2).
239 = disconnect, 238 = works

Just though you guys would want to know.

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by dr3w2 on Sat, 06 Feb 2010 23:12:08 GMT
View Forum Message <> Reply to Message

Just to add to this, to my recollection this does actually crash the server. If you do a !msg with this length of characters the actual FDS restarts

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by GEORGE ZIMMER on Sun, 07 Feb 2010 01:31:01 GMT
View Forum Message <> Reply to Message

Yeah, would be nice to see certain things like this being un-capped, or atleast set to a really high number.

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by Jerad2142 on Sun, 07 Feb 2010 04:06:34 GMT
View Forum Message <> Reply to Message

andr3w282 wrote on Sat, 06 February 2010 16:12Just to add to this, to my recollection this does actually crash the server. If you do a !msg with this length of characters the actual FDS restarts
Well it kicks everyone, so does it crash or just start a new map?

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by StealthEye on Sun, 07 Feb 2010 17:50:19 GMT
View Forum Message <> Reply to Message

There are several issues with long messages. First the message length can't exceed 0x100 = 256 characters. (you probably found 238 because there are additional headers prepended or w/e). Additionally the total packet (packet type, message type, sender, message, etc.) can not exceed 548 bytes. I think messages are sent as wide char strings, meaning the total message length can still not exceed 274-(1/2 bytes needed for additional headers) characters even if we enlarge the 0x100 limit. This means the extra space gained by doing so would be marginal. Lifting the 548 is

atm not possible afaik, because we do not own all places that touch packets. Cloning all these is probably a lot of work.

Best we can do atm is probably to avoid clients crashing when these messages are sent, or avoid sending messages of this length at all.

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by dr3w2 on Sun, 07 Feb 2010 19:48:24 GMT
View Forum Message <> Reply to Message

StealthEye wrote on Sun, 07 February 2010 17:50There are several issues with long messages. First the message length can't exceed 0x100 = 256 characters. (you probably found 238 because there are additional headers prepended or w/e). Additionally the total packet (packet type, message type, sender, message, etc.) can not exceed 548 bytes. I think messages are sent as wide char strings, meaning the total message length can still not exceed 274-(1/2 bytes needed for additional headers) characters even if we enlarge the 0x100 limit. This means the extra space gained by doing so would be marginal. Lifting the 548 is atm not possible afaik, because we do not own all places that touch packets. Cloning all these is probably a lot of work.

Best we can do atm is probably to avoid clients crashing when these messages are sent, or avoid sending messages of this length at all.
Makes sense to me and yeah I doubt that would be worth the trouble at all. Go with the check the length before executing

---

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by GEORGE ZIMMER on Sun, 07 Feb 2010 21:24:37 GMT
View Forum Message <> Reply to Message

StealthEye wrote on Sun, 07 February 2010 11:50There are several issues with long messages. First the message length can't exceed 0x100 = 256 characters. (you probably found 238 because there are additional headers prepended or w/e). Additionally the total packet (packet type, message type, sender, message, etc.) can not exceed 548 bytes. I think messages are sent as wide char strings, meaning the total message length can still not exceed 274-(1/2 bytes needed for additional headers) characters even if we enlarge the 0x100 limit. This means the extra space gained by doing so would be marginal. Lifting the 548 is atm not possible afaik, because we do not own all places that touch packets. Cloning all these is probably a lot of work.

Best we can do atm is probably to avoid clients crashing when these messages are sent, or avoid sending messages of this length at all.
Would it be possible to check the length, and if it's too big, cut it into several messages?

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by Gen_Blacky on Sun, 07 Feb 2010 22:15:06 GMT

View Forum Message <> Reply to Message

GEORGE ZIMMER wrote on Sun, 07 February 2010 15:24StealthEye wrote on Sun, 07 February 2010 11:50There are several issues with long messages. First the message length can't exceed 0x100 = 256 characters. (you probably found 238 because there are additional headers prepended or w/e). Additionally the total packet (packet type, message type, sender, message, etc.) can not exceed 548 bytes. I think messages are sent as wide char strings, meaning the total message length can still not exceed 274-(1/2 bytes needed for additional headers) characters even if we enlarge the 0x100 limit. This means the extra space gained by doing so would be marginal. Lifting the 548 is atm not possible afaik, because we do not own all places that touch packets. Cloning all these is probably a lot of work.

Best we can do atm is probably to avoid clients crashing when these messages are sent, or avoid sending messages of this length at all.
Would it be possible to check the length, and if it's too big, cut it into several messages?

what do you mean several msgs.

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by TruYuri on Mon, 08 Feb 2010 00:56:21 GMT
View Forum Message <> Reply to Message

Gen_Blacky wrote on Sun, 07 February 2010 17:15
what do you mean several msgs.

User types:
"this message is too long"

Game displays:
"this message is too "
"long"

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by GEORGE ZIMMER on Mon, 08 Feb 2010 04:32:54 GMT
View Forum Message <> Reply to Message

TruYuri wrote on Sun, 07 February 2010 18:56Gen_Blacky wrote on Sun, 07 February 2010 17:15
what do you mean several msgs.

User types:
"this message is too long"

Game displays:
"this message is too "
"long"

Exactly.

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by Sladewill on Mon, 08 Feb 2010 09:00:03 GMT
View Forum Message <> Reply to Message

yes it can be done quite easily.

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by StealthEye on Mon, 08 Feb 2010 10:27:54 GMT
View Forum Message <> Reply to Message

That's up to the (user/)bot. There are multiple ways to split messages up, such as

Host: (StealthEye@IRC) This message is ...
Host: ... too long.

or

Host: (StealthEye@IRC) This message is too
Host: (StealthEye@IRC) long.

or some combination or whatever. It may even be necessary to avoid misinterpretation such as

"This message is too !kick blah"
Host: (StealthEye@IRC) This message is too
Host: !kick blah

We'll leave it up to the bot to determine the preferred split style. We will most likely only fix the crashes.

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by Jerad2142 on Wed, 10 Feb 2010 16:22:23 GMT
View Forum Message <> Reply to Message

I just say you guys make the function go though something like this.

```
void Send_Message_Player(GameObject *o,float red,float green,float blue,const char *msg);
{
   Text[238];
   sprintf(Text,"%s",msg);
   *DisplayToPlayerCode*(Text);
}
```

I'd assume you guys would fix the problem with something simple like that, but really have no clue as bhs.dll isn't open source.

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by StealthEye on Wed, 10 Feb 2010 17:37:17 GMT
View Forum Message <> Reply to Message

We would probably fix it on a lower level, at the netcode level where this bug is actually caused. It's likely that we will simply cut it off at the maximum amount of characters rather than splitting it or blocking it entirely since this is much easier at this level. We should do it low level because Send_Message_Player is definitely not the only function suffering from the same bug.

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by Sladewill on Wed, 10 Feb 2010 23:23:52 GMT
View Forum Message <> Reply to Message

hmm i might be getting this, could this be caused by too many messages being sent to server at same time?

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by Jerad2142 on Thu, 11 Feb 2010 15:44:30 GMT
View Forum Message <> Reply to Message

Sladewill wrote on Wed, 10 February 2010 16:23hmm i might be getting this, could this be caused by too many messages being sent to server at same time?
Right now its going to be a message size issue more then a number, beings I first noticed the issue in 1vs1 lan, it would have only been sending the message to 1 other player. If it was a number of messages issue, every server would crash when a message was sent with any number of players. If it was a number of players issue combined with message size, then as you got more players in game you would have to make the message shorter and shorter in order to not disconnect the clients. To my knowledge this is not the case 238 is the length needed to disconnect the clients regardless how many players are in game.

Subject: Re: 3.4.4 Send_Message_Player Disconnect
Posted by StealthEye on Thu, 11 Feb 2010 16:38:15 GMT
View Forum Message <> Reply to Message

Pretty close, but again, 238 is not the limit. Depending on the color it may be larger than that. The real limit is 256, but consider the following overhead:

256 -
10 bytes default overhead

1-3 bytes for red
1-3 bytes for green
1-3 bytes for blue

The color components are sent as string, therefore 0-9 take 1 byte, 10-99 take 2 and 100-255 take 3. If you write a message in black, you will therefore have a higher "message limit".

It would be safest not to send messages longer than 256-10-3-3-3 = 237 bytes. Although apparently 238 worked for you, it is not guaranteed to work in every situation, therefore you best avoid sending messages longer than 237 bytes.
