Subject: New FDS exploit fix (players can use admin commands)
Posted by TimeFX on Thu, 28 Jul 2005 23:24:57 GMT
View Forum Message <> Reply to Message

While going through linux server code I found a function what allows players to execute any console command on the server. For example every player can kick every other player on the server, players can send host message, players can shutdown the server and so on.

I made the patch for linux RH7 & RH8 and Windows dedicated server. Patching the windows game client isn't possible since RenGuard would disallow the change. I compiled the linux binary under SuSE 9.2 - hope it works.

Remember: You should make a backup of your renegade binary before patching.
To use the patch use "./rr_patch01 <your binary>"
Using the patch again will remove the changes.

Linux patcher: http://www.icefinch.net/rr/rr_patch01
Windows patcher: http://www.icefinch.net/rr/rr_patch01.exe

If you experience crashes after patching (which shouldn't happen) please report me your FDS version and the address where the crash occurred.

Greets,
TimeFX

IMPORTANT NOTE:
RenGuard 1.03 does NOT protect you from this exploit.

EDIT
This patch is CP1 compatible.

RH8: successfully tested
RH7: no feedback
WIN: no feedback

Subject: Re: New FDS exploit fix (players can use admin commands)
Posted by =HT=T-Bird on Thu, 28 Jul 2005 23:36:34 GMT
View Forum Message <> Reply to Message

Nice Catch! Looks like a good fix to stick in SSCP2. (once it gets some testing, of course)

Subject: Re: New FDS exploit fix (players can use admin commands)
Posted by TimeFX on Thu, 28 Jul 2005 23:45:07 GMT
View Forum Message <> Reply to Message

=HT=T-Bird wrote on Fri, 29 July 2005 01:36Nice Catch! Looks like a good fix to stick in SSCP2. (once it gets some testing, of course)

Thanks

The exploit works in both directions, so server admins could execute console commands at the player's win client.
So they should fix that in client CP too

But why waiting for SSCP2?

PS: Westwood sucks for adding this 'feature'...

Subject: Re: New FDS exploit fix (players can use admin commands)
Posted by Cat998 on Fri, 29 Jul 2005 00:31:04 GMT
View Forum Message <> Reply to Message

Good job !

Subject: Re: New FDS exploit fix (players can use admin commands)
Posted by jonwil on Fri, 29 Jul 2005 00:31:53 GMT
View Forum Message <> Reply to Message

Well it just so happens that scripts.dll/bhs.dll 2.1.3 (which will be out as soon as I fix a few things) will disable these network events on both the client and the server (and a few others too)

Subject: Re: New FDS exploit fix (players can use admin commands)
Posted by Cat998 on Fri, 29 Jul 2005 00:34:39 GMT
View Forum Message <> Reply to Message

jonwil wrote on Thu, 28 July 2005 20:31Well it just so happens that scripts.dll/bhs.dll 2.1.3 (which will be out as soon as I fix a few things)
will disable these network events on both the client and the server (and a few others too)

Who wants to wait ?
timefx already fixed it

Subject: Re: New FDS exploit fix (players can use admin commands)
Posted by Renx on Fri, 29 Jul 2005 15:52:25 GMT
View Forum Message <> Reply to Message

wow, I had no idea we were so vulnerable. Thanks for the fix dude!

Subject: Re: New FDS exploit fix (players can use admin commands)
Posted by Renerage on Wed, 17 Aug 2005 07:15:56 GMT
View Forum Message <> Reply to Message

that explains alot...

Subject: Re: New FDS exploit fix (players can use admin commands)
Posted by DarkComet on Wed, 07 Dec 2005 13:56:12 GMT
View Forum Message <> Reply to Message

thanks