Runtime Infrastructure - Bug #7498

allow a single Web client launch if the client presses ENTER key multiple times

07/11/2023 05:04 AM - Constantin Asofiei

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
billable:	No	**case_num:**	
vendor_id:	GCD	**version:**	

Description

Related issues:

Related to User Interface - Bug #3304: Eliminate denial of service in virtual...	**New**	**06/26/2017**
Related to Runtime Infrastructure - Bug #30: detect denial of service attempt...	**New**	

History

#2 - 07/11/2023 05:07 AM - Constantin Asofiei

In the FWD Web client login page, if the FWD client presses the ENTER key multiple times, each keystroke will be posted to the FWD server; this in turn will try to launch a client for each case.

In #7479, a protection was added to allow the FWD server to 'self heal' if the FWD client fails to start completely; previously, a config resource (which includes the Web port for the FWD client jetty web server) remained 'in use' and never re-allocated, ending up in a 'no ports available' scenario.

The caveat with the changes in #7479 is this: it will take 30 seconds (or the watchdog timer value, whichever is higher) for the FWD server to 'self heal'. But, if a user spams the ENTER key in the Web client login form, there is nothing preventing a 'small denial-of-service' happening. I don't know how to protect against this.

This task is meant to add protection code on server-side, to allow only the first submit to go through.

#3 - 08/02/2023 08:26 AM - Constantin Asofiei

- Related to Bug #3304: Eliminate denial of service in virtual desktop mode added

#4 - 11/07/2023 07:37 AM - Galya B

With trunk r14783 (3931a merged) default login page has a 'Sign In' button, that gets disabled on the first click, until a response is returned. This is client-side protection and prevents unintentional DOS.

The server-side protection lies in the essence of SSO. If SSO is implemented and enabled, the client process launches only after the in-app user is authenticated, so the offender can be easily identified. Also SsoAuthenticator implementation can deny access if the customer decides to keep track of the frequency of sign-ins. It's in the hands of the customers to apply such DOS protection.

#5 - 11/07/2023 07:38 AM - Galya B

- Related to Bug #30: detect denial of service attempt and try to reduce the impact added