VRSpace.org - Support #67

VAS

05/13/2021 07:45 PM - Josip Almasi

Status:	Feedback	**Start date:**	05/13/2021
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour
Description			

History

#1 - 05/13/2021 07:45 PM - Josip Almasi

- Status changed from New to In Progress

#2 - 05/25/2021 11:25 AM - Josip Almasi

Server secure enough to prevent peer exploits.
Clients not closing connection (SYN) may cause resource leaks. TODO: tcp keepalive

#3 - 06/09/2021 12:41 PM - Josip Almasi

Practical websocket connection limit around 5000. DoS potential. Best protection at reverse proxy.
https://serverfault.com/questions/252555/limit-simultaneous-connections-per-ip-with-apache2

The defaults are maxConnections=10,000 and maxThreads=200
https://stackoverflow.com/questions/24678661/tomcat-maxthreads-vs-maxconnections
https://stackoverflow.com/questions/39644830/what-are-acceptcount-maxconnections-and-maxthreads-in-tomcat-http-connector-con

Implement local per-client connection limit in SessionManager.afterConnectionEstablished(), using session.getRemoteAddress()

#4 - 07/05/2021 01:22 PM - Josip Almasi

- File vrspace-report-20210703.zip added

- Status changed from In Progress to Feedback

Denial of service through resource exhaustion [MEDIUM]
It is possible to use all websockets from a single source.
• Components with known vulnerabilities [LOW]
Application uses several older version of dependencies that have since been
updated due to vulnerabilities found in them:
- jquery version 3.3.1.min
- bcprov-jdk15on-1.64
- neo4j-java-driver-4.0.2
- Spring-core-5.2.14
• Parameter injection [LOW]
It is possible to inject parameter pair [“parameter”:”value”] that will be
forwarded to other clients within the same world.

Files

vrspace-report-20210703.zip	1.67 MB	07/05/2021	Josip Almasi