

Commit 7dd54c2

Browse files

consideRatio authored 4 days ago · 6 / 6 · Verified

Merge pull request [#151](#) from consideRatio/pr/verify-port
Ensure TigerVNC isn't accessible via the network

main (#151) · v3.0.1 2 parents [5a46ef7](#) + [127dbb2](#) commit 7dd54c2

Filter files...

- ▼ .github/workflows
 - test.yaml
 - .gitignore
- ▼ jupyter_remote_desktop_proxy
 - setup_websockify.py

3 files changed +42 -3 lines changed Search within code

.github/workflows/test.yaml +21 -2

```
@@ -60,7 +60,13 @@ jobs:
60 60
61 61     - name: Test vncserver
62 62       run: |
63       - container_id=$(docker run -d -it -p 5901:5901 test vncserver -xstartup
        /opt/install/jupyter_remote_desktop_proxy/share/xstartup -verbose -fg -geometry 1680x1050
        -SecurityTypes None -rfbport 5901)
63 +         # TigerVNC needs to be configured with -rfbport -1 to not open a TCP
64 +         # port, while TurboVNC doesn't support being passed -1 and won't open
65 +         # a TCP port anyhow.
66 +         rfbport_arg="-rfbport -1"
67 +         if [ "${{ matrix.vncserver }}" == "turbovnc" ]; then rfbport_arg=""; fi
68 +
69 +         container_id=$(docker run -d -it test vncserver -xstartup
        /opt/install/jupyter_remote_desktop_proxy/share/xstartup -verbose -fg -geometry 1680x1050
        -SecurityTypes None -rfbunixpath /tmp/vncserver.socket $rfbport_arg)
```

```

64 70          sleep 1
65 71
66 72          echo "::group::Install netcat, a test dependency"
❧ @@ -70,9 +76,18 @@ jobs:
70 76          '
71 77          echo "::endgroup::"
72 78
73 79 -          docker exec -it $container_id timeout --preserve-status 1 nc -v localhost 5901
      2>&1 | tee -a /dev/stderr | \
79 80 +          docker exec -it $container_id timeout --preserve-status 1 nc -vU
      /tmp/vncserver.socket 2>&1 | tee -a /dev/stderr | \
74 81          grep --quiet RFB && echo "Passed test" || { echo "Failed test" &&
      TEST_OK=false; }
75 82 +          echo "::group::Security - Verify TCP ports wasn't opened"
83 83 +          ports=(5800 5801 5900 5901)
84 84 +          for port in "${ports[@]}"
85 85 +          do
86 86 +          docker exec -it $container_id timeout --preserve-status 1 nc -vz localhost
      $port | tee -a /dev/stderr | \
87 87 +          grep --quiet succeeded && { echo "Failed security check - port $port
      open" && SECURITY_OK=false; } || echo "Passed security check - port $port not opened"
88 88 +          done
89 89 +          echo "::endgroup::"
90 90 +
76 91          echo "::group::vncserver logs"
77 92          docker exec $container_id bash -c 'cat ~/.vnc/*.log'
78 93          echo "::endgroup::"
❧ @@ -82,6 +97,10 @@ jobs:
82 97          echo "Test failed!"
83 98          exit 1
84 99      fi
100 100 +          if [ "$SECURITY_OK" == "false" ]; then
101 101 +          echo "Security check failed!"
102 102 +          exit 1
103 103 +          fi
85 104
86 105      - name: Install playwright
87 106          run: |

```

```

1 1 # Extra ignore patterns specific to this project
2 2 # Installed JS libraries
3 3 node_modules/
4 4 + package-lock.json
4 5 # Built JS files
5 6 jupyter_remote_desktop_proxy/static/dist
6 7

```



jupyter_remote_desktop_proxy/setup_websockify.py

+20
-1
□□□□□
□
...

```

@@ -12,8 +12,27 @@ def setup_websockify():
12 12         "vncserver executable not found, please install a VNC server"
13 13     )
14 14
15 15 +     # TurboVNC and TigerVNC share the same origin and both use a Perl script
16 16 +     # as the executable vncserver. We can determine if vncserver is TigerVNC
17 17 +     # by searching tigervnc string in the Perl script.
18 18 +     #
19 19 +     # The content of the vncserver executable can differ depending on how
20 20 +     # TigerVNC and TurboVNC has been distributed. Below are files known to be
21 21 +     # read in some situations:
22 22 +     #
23 23 +     # - https://github.com/TigerVNC/tigervnc/blob/v1.13.1/unix/vncserver/vncserver.in
24 24 +     # - https://github.com/TurboVNC/turbovnc/blob/3.1.1/unix/vncserver.in
25 25 +     #
26 26 +     with open(vncserver) as vncserver_file:
27 27 +         vncserver_file_text = vncserver_file.read().casefold()
28 28 +         is_turbovnc = "turbovnc" in vncserver_file_text
29 29 +
15 30     # {unix_socket} is expanded by jupyter-server-proxy
16 31 -     vnc_args = [vncserver, '-rfbunixpath', '{unix_socket}']
31 31 +     vnc_args = [vncserver, '-rfbunixpath', "{unix_socket}", "-rfbport", "-1"]
32 32 +     if is_turbovnc:
33 33 +         # turbovnc doesn't handle being passed -rfbport -1, but turbovnc also
34 34 +         # defaults to not opening a TCP port which is what we want to ensure
35 35 +         vnc_args = [vncserver, '-rfbunixpath', "{unix_socket}"]
17 36
18 37     xstartup = os.getenv("JUPYTER_REMOTE_DESKTOP_PROXY_XSTARTUP")
19 38     if not xstartup and not os.path.exists(os.path.expanduser('~/.vnc/xstartup')):

```



Comments 0



Please [sign in](#) to comment.