

TigerVNC accessible via the network and not just via a UNIX socket as intended

Critical

consideRatio published **GHSA-vrq4-9hc3-cgp7** 4 days ago

Package	Affected versions	Patched versions
 jupyter-remote-desktop-proxy (pip)	3.0.0	>=3.0.1

Severity

Critical

 9.0 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Adjacent
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	None
User interaction	None

Vulnerable System Impact Metrics

Confidentiality	High
Integrity	High
Availability	High

Subsequent System Impact Metrics

Confidentiality	High
Integrity	High
Availability	High

[Learn more about base metrics](#)

Description

Summary

jupyter-remote-desktop-proxy was meant to rely on UNIX sockets readable only by the current user since version 3.0.0, but when used with TigerVNC, the VNC server started by jupyter-remote-desktop-proxy were still accessible via the network.

This vulnerability does not affect users having TurboVNC as the vncserver executable.

Credits

This vulnerability was identified by Arne Gottwald at University of Göttingen and analyzed, reported, and reviewed by [@frejanordsiek](#).

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H




CVE ID

CVE-2025-32428

Weaknesses

CWE-668

Credits

-  **frejanordsiek** Analyst
-  Remediation developer
consideratio
-  Remediation reviewer
minrk