CORS Origin Validation Bypass via `re.match()` in `allow_origin_pat`

Moderate **Yann-P** published **GHSA-24qx-w28j-9m6p** 8 hours ago

Package

jupyter-server (pip)

Affected versions

<=2.17.0

Patched versions

2.18.0

Description

Jupyter Server uses `re.match()` to validate the Origin header against the `allow_origin_pat` configuration.

Since `re.match()` only anchors at the start of the string, an attacker who controls a domain like `http://trusted.example.com.evil.com/` passes validation against a pattern intended to match only `trusted.example.com`.

Impact

<=2.17.0

Patches

`057869a`, `49b3439`

Workarounds

Wrap your `allow_origin_pat` value with `^` and `$`

References

#603
https://docs.python.org/3/library/re.html#re.fullmatch
https://docs.python.org/3/library/re.html#re.match

Severity

Moderate 5.9 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	None
User interaction	Active
Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	Low
Availability	None
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-40110

Weaknesses

▶ CWE-777

Credits

 **vnykmshr** Reporter

 **Yann-P** Remediation developer