

[jupyter-server](#) / [jupyter\\_server](#) Public[Code](#) [Issues](#) 193 [Pull requests](#) 31 [Discussions](#) [Actions](#) [Projects](#)

# Open redirection vulnerability in `next` query parameter

Moderate Yann-P published [GHSA-qh7q-6qm3-653w](#) 7 hours ago

## Package

 [jupyter\\_server](#) (pip)

### Affected versions

&lt;=2.17.0

### Patched versions

2.18.0

## Description

### Summary

The `?next=...` URL query parameter has an open redirection vulnerability. In `jupyter_server<=2.17.0`, this URL query parameter allows redirection to arbitrary external domains, which can be exploited to facilitate phishing attacks on server users.

### Details

The vulnerability is caused by insufficient validation in the `LoginFormHandler._redirect_safe()` method.

- Source code reference:

[jupyter\\_server/jupyter\\_server/auth/login.py](#)Lines 33 to 76 in [987ebdd](#)

```
33     def _redirect_safe(self, url, default=None):
34         """Redirect if url is on our PATH
35
36         Full-domain redirects are allowed if they pass our CORS origin check
37
38         Otherwise use default (self.base_url if unspecified).
39         """
40         if default is None:
41             default = self.base_url
42         # protect chrome users from mishandling unescaped backslashes.
```

```
43         # \ is not valid in urls, but some browsers treat it as /
44         # instead of %5C, causing `\\` to behave as `//`
```

This vulnerability was originally reported by Noriaki Iwasaki. All discovery credit goes to them.

## PoC

1. Navigate to `http://localhost:8888/login?next=///google.com`
2. Observe that the user is redirected to `google.com` despite it being an external domain.

The external domain passed in the `?next` parameter may be replaced with a malicious lookalike to facilitate phishing attacks. Jupyter Server deployments served on a public domain are especially vulnerable, as `prod.company.com` may be redirected to a look-alike URL such as `prod.company.dev`.

## Impact

This vulnerability affects all users, especially enterprise users who work with sensitive/confidential data.

## Patches

Jupyter Server 2.18+

## Workaround

None.

## Severity

Moderate 6.0 / 10

### CVSS v4 base metrics

#### Exploitability Metrics

Attack Vector	Local
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User interaction	Passive

#### Vulnerable System Impact Metrics

Confidentiality	None
Integrity	None
Availability	None

#### Subsequent System Impact Metrics

Confidentiality	High
Integrity	None
Availability	None
<a href="#">Learn more about base metrics</a>	

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

### CVE ID

CVE-2025-61669

### Weaknesses

► CWE-601

### Credits

 <b>dlqqq</b>	Remediation developer
 <b>niwasak1</b>	Finder
 <b>Yann-P</b>	Coordinator
 <b>Carreau</b>	Coordinator