Command linker attributes chained with help command enable one-click authentication token theft

High **krassowski** published **GHSA-rch3-82jr-f9w9** last week

Package

@jupyter-notebook/help-extension (npm)

Affected versions	Patched versions
>=7.0.0,<= 7.5.5	7.5.6

@jupyterlab/help-extension (npm)

<=4.5.6	4.5.7

jupyterlab (pip)

<=4.5.6	4.5.7

notebook (pip)

>=7.0.0,<= 7.5.5	7.5.6

Description

Impact

A stored Cross-Site Scripting (XSS) vulnerability in Jupyter Notebook allows attackers to steal authentication tokens from users who open malicious notebook files and interact with elements that the attacker can make look indistinguishable from legitimate controls (single click interaction).

The vulnerability enables complete account takeover through the Jupyter REST API, allowing the attacker to:

1. Read all files
2. Modify/create files
3. Access running kernels and execute arbitrary code

4. Create terminals for shell access

Patches

Jupyter Notebook 7.5.6 and JupyterLab 4.5.7 include patches for this vulnerability.

Workarounds

The help extension can be disabled via CLI:

```
jupyter labextension disable @jupyter-notebook/help-extension
jupyter labextension disable @jupyterlab/help-extension
```

Hardening

The patched versions include a toggle to disable the command linker functionality altogether, for example via `overrides.json`:

```
{
  "@jupyterlab/apputils-extension:sanitizer": {
    "allowCommandLinker": false
  }
}
```

References

- https://jupyterlab.readthedocs.io/en/latest/user/commands.html#commands-in-markdown-output-and-files

Acknowledgments

Reported by Daniel Teixeira - NVIDIA AI Red Team

Severity

High 8.4 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None

Privileges Required	High
User interaction	Active
Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-40171

Weaknesses

- CWE-79
- CWE-601

Credits

dtrops	Reporter
Carreau	Coordinator
Yann-P	Coordinator
krassowski	Coordinator
jtpio	Remediation reviewer