



CVE-2021-32797

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-32797
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-09 21:15:00 UTC
Updated	2022-04-07 18:40:00 UTC
Description	JupyterLab is a user interface for Project Jupyter which will eventually replace the classic Jupyter Notebook. In affected ver

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jupyter	Jupyterlab	All	All	All	All
Application	Jupyter	Jupyterlab	-	All	All	All

References

Reference	Source	L
JupyterLab: XSS due to lack of sanitization of the action attribute of an HTML form · Advisory · jupyterlab/jupyterlab · GitHub	CONFIRM	g
Merge pull request from GHSA-4952-p58q-6crx · jupyterlab/jupyterlab@5048259 · GitHub	MISC	g
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[980395](#) Python (pip) Security Update for notebook (GHSA-4952-p58q-6crx)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)