



CVE-2018-21030

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

Summary

CVE	CVE-2018-21030
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-31 15:15:00 UTC
Updated	2020-11-19 07:15:00 UTC
Description	Jupyter Notebook before 5.5.0 does not use a CSP header to treat served files as belonging to a separate origin. Thus, for

Risk And Classification

Problem Types: CWE-79 | CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jupyter	Notebook	All	All	All	All
Application	Jupyter	Notebook	All	All	All	All

References

Reference	Source
[SECURITY] [DLA 2432-1] jupyter-notebook security update	MLIST
Release 5.5.0 · jupyter/notebook · GitHub	MISC
Use CSP header to treat served files as belonging to a separate origin by takluyver · Pull Request #3341 · jupyter/notebook · GitHub	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[198916](#) Ubuntu Security Notification for Jupyter Notebook Vulnerabilities (USN-5585-1)

[982600](#) Python (pip) Security Update for notebook (GHSA-jqwc-jm56-wcwj)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)