



# CVE-2022-0427

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

## Summary

<b>CVE</b>	CVE-2022-0427
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@gitlab.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-28 19:15:00 UTC
<b>Updated</b>	2022-04-04 19:16:00 UTC
<b>Description</b>	Missing sanitization of HTML attributes in Jupyter notebooks in all versions of GitLab CE/EE since version 14.5 allows an at

## Risk And Classification

**Problem Types:** CWE-352

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Gitlab</a>	<a href="#">Gitlab</a>	All	All	All	All
Application	<a href="#">Gitlab</a>	<a href="#">Gitlab</a>	All	All	All	All

## References

Reference	Source
Arbitrary POST request as victim user from HTML injection in Jupyter notebooks (#347284) · Issues · GitLab.org / GitLab · GitLab	MISC
HackerOne	MISC
2022/CVE-2022-0427.json · master · GitLab.org / cves · GitLab	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Thanks [joaxcar](https://hackerone.com/joaxcar) for reporting this vulnerability through our HackerOne bug bounty program

## Legacy QID Mappings

© [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](#)