



# CVE-2021-45326

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

## Summary

<b>CVE</b>	CVE-2021-45326
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-08 15:15:00 UTC
<b>Updated</b>	2022-02-11 17:03:00 UTC
<b>Description</b>	Cross Site Request Forgery (CSRF) vulnerability exists in Gitea before 1.5.2 via API routes. This can be dangerous especially if the user is authenticated.

## Risk And Classification

**Problem Types:** CWE-352

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gitea	Gitea	All	All	All	All

## References

Reference	Source	Link
Enforce token on api routes [fixed critical security issue #4357] by beeonthego · Pull Request #4840 · go-gitea/gitea · GitHub	MISC	<a href="#">g</a>
[Proposal] CSRF checks on GET routes · Issue #4838 · go-gitea/gitea · GitHub	MISC	<a href="#">g</a>
Gitea 1.5.2 is released - Blog	MISC	<a href="#">b</a>
CVE Program record	CVE.ORG	<a href="#">v</a>
NVD vulnerability detail	NVD	<a href="#">n</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

502294 Alpine Linux Security Update for gitea

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](#).

**Free CVE JSON API** [cve.report/api](#)

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