



CVE-2022-42968

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

Summary

CVE	CVE-2022-42968
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-16 04:15:00 UTC
Updated	2022-12-03 01:35:00 UTC
Description	Gitea before 1.17.3 does not sanitize and escape refs in the git backend. Arguments to git commands are mishandled.

Risk And Classification

Problem Types: CWE-88

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
Release v1.17.3 · go-gitea/gitea · GitHub	MISC	github.com
Sanitize and Escape refs in git backend (#21464) by 6543 · Pull Request #21463 · go-gitea/gitea · GitHub	MISC	github.com
Gitea: Multiple Vulnerabilities (GLSA 202210-14) — Gentoo security	GENTOO	security.gentoo.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[502856](#) Alpine Linux Security Update for gitea

[505740](#) Alpine Linux Security Update for gitea

[710660](#) Gentoo Linux Gitea Multiple Vulnerabilities (GLSA 202210-14)

© [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](#)