



CVE-2023-0957

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

Summary

CVE	CVE-2023-0957
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-03 08:15:00 UTC
Updated	2023-03-10 19:04:00 UTC
Description	An issue was discovered in Gitpod versions prior to release-2022.11.2.16. There is a Cross-Site WebSocket Hijacking (CSW

Risk And Classification

Problem Types: CWE-346

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Gitpod remote code execution 0-day vulnerability via WebSockets Snyk	MISC	snyk.io
[public-api-server] Forward Origin header where provided by geropl · Pull Request #16405 · gitpod-io/gitpod · GitHub	MISC	github.cc
[server] strict same site origin for /api/gitpod endpoint · gitpod-io/gitpod@1295698 · GitHub	MISC	github.cc
Gitpod Trust Center SafeBase	MISC	app.safe
[server] strict same site origin for /api/gitpod endpoint by akosyakov · Pull Request #16378 · gitpod-io/gitpod · GitHub	MISC	github.cc
Release 2022.11.2 · gitpod-io/gitpod · GitHub	MISC	github.cc
Use context to store and populate origin · gitpod-io/gitpod@673ab68 · GitHub	MISC	github.cc
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

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

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