



CVE-2021-25924

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

Summary

CVE	CVE-2021-25924
State	PUBLIC
Assigner	vulnerabilitylab@whitesourcesoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-01 18:15:00 UTC
Updated	2023-11-07 03:31:00 UTC
Description	In GoCD, versions 19.6.0 to 21.1.0 are vulnerable to Cross-Site Request Forgery due to missing CSRF protection at the `/g

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Thoughtworks	GoCd	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2021-25924 WhiteSource Vulnerability Database		www.whitesourcesoftware.com	
CVE-2021-25924 WhiteSource Vulnerability Database	MISC	www.whitesourcesoftware.com	
#000 - Add missing Content-Type check · gocd/gocd@7d0baab · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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