CVE-2020-5415

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-5415
State	PUBLIC
Assigner	security@pivotal.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-12 17:15:00 UTC
Updated	2020-08-19 14:04:00 UTC
Description	Concourse, versions prior to 6.3.1 and 6.4.1, in installations which use the GitLab auth connector, is vulnerable to identity s

Risk And Classification

Problem Types: CWE-290

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pivotal Software	Concourse	All	All	All	All
Application	Pivotal Software	Concourse	All	All	All	All

References

Reference	Source
CVE-2020-5415: Concourse's GitLab auth allows impersonation | Security | VMware Tanzu	CONFIRM
GitLab auth uses full name instead of username as user ID, allowing impersonation · Advisory · concourse/concourse · GitHub	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report