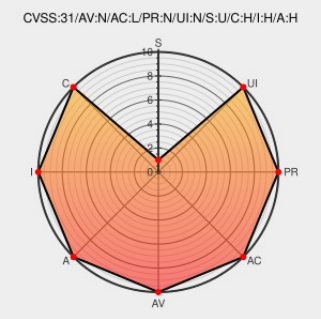
CVE-2021-22869

Published on: 09/24/2021 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:30:00 AM UTC

CVE-2021-22869

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Enterprise Server from Github contain the following vulnerability:

An improper access control vulnerability in GitHub Enterprise Server allowed a workflow job to execute in a self-hosted runner group it should not have had access to. This affects customers using self-hosted runner groups for access control. A repository with access to one enterprise runner group could access all of the enterprise runner groups within the organization because of improper authentication checks during the request. This could cause code to be run unintentionally by the incorrect runner group. This vulnerability affected GitHub Enterprise Server versions from 3.0.0 to 3.0.15 and 3.1.0 to 3.1.7 and was fixed in 3.0.16 and 3.1.8 releases.

CVE-2021-22869 has been assigned by product-cna@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **GitHub** - **GitHub Enterprise Server** version **< 3.0.16**

Affected Vendor/Software: **GitHub** - **GitHub Enterprise Server** version **< 3.1.8**

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Release notes - GitHub Docs	docs.github.com text/html	MISC docs.github.com/en/enterprise-server@3.0/admin/release-notes#3.0.16
Release notes - GitHub Docs	docs.github.com text/html	MISC docs.github.com/en/enterprise-server@3.1/admin/release-notes#3.1.8

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Github	Enterprise Server	All	All	All	All

cpe:2.3:a:github:enterprise_server:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-22869 : An improper access control vulnerability in GitHub Enterprise Server allowed a workflow job to exe… twitter.com/i/web/status/1…	2021-09-24 17:55:21
@0_exploit	CVE-2021-22869 dlvr.it/S8H1kJ	2021-09-24 22:49:03
@SecRiskRptSME	RT: CVE-2021-22869 An improper access control vulnerability in GitHub Enterprise Server allowed a workflow job to… twitter.com/i/web/status/1…	2021-09-25 07:33:22
@threatmeter	CVE-2021-22869 An improper access control vulnerability in GitHub Enterprise Server allowed a workflow job to execu… twitter.com/i/web/status/1…	2021-09-25 09:09:51

← Previous ID

Next ID→

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