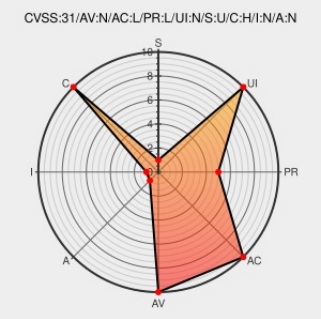
CVE-2021-22862

Published on: 03/02/2021 12:00:00 AM UTC

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

CVE-2021-22862

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



Certain versions of Github from Github contain the following vulnerability:

An improper access control vulnerability was identified in GitHub Enterprise Server that allowed an authenticated user with the ability to fork a repository to disclose Actions secrets for the parent repository of the fork. This vulnerability existed due to a flaw that allowed the base reference of a pull request to be updated to point to an arbitrary SHA or another pull request outside of the fork repository. By establishing this incorrect reference in a PR, the restrictions that limit the Actions secrets sent a workflow from forks could be bypassed. This vulnerability affected GitHub Enterprise Server version 3.0.0, 3.0.0.rc2, and 3.0.0.rc1. This vulnerability was reported via the GitHub Bug Bounty program.

CVE-2021-22862 has been assigned by product-cna@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **GitHub** - **GitHub Enterprise Server** version **< 3.0.1**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

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#3.0.1

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	Github	3.0.0	-	All	All
Application	Github	Github	3.0.0	rc1	All	All
Application	Github	Github	3.0.0	rc2	All	All
Application	Github	Github	3.0.0	-	All	All
Application	Github	Github	3.0.0	rc1	All	All
Application	Github	Github	3.0.0	rc2	All	All

cpe:2.3:a:github:github:3.0.0:-:*:*:*:*:*:*:

cpe:2.3:a:github:github:3.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:github:github:3.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:github:github:3.0.0:-:*:*:*:*:*:*:

cpe:2.3:a:github:github:3.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:github:github:3.0.0:rc2:*:*:*:*:*:*:

Discovery Credit

Teddy Katz

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

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