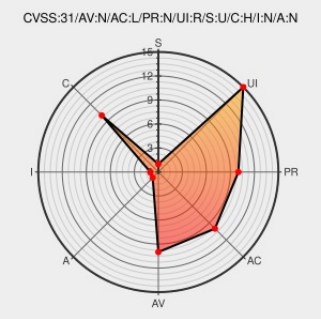
CVE-2021-22865

Published on: 04/02/2021 12:00:00 AM UTC

Last Modified on: 10/25/2022 02:04:00 PM UTC

CVE-2021-22865

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



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

An improper access control vulnerability was identified in GitHub Enterprise Server that allowed access tokens generated from a GitHub App's web authentication flow to read private repository metadata via the REST API without having been granted the appropriate permissions. To exploit this vulnerability, an attacker would need to create a GitHub App on the instance and have a user authorize the application through the web authentication flow. The private repository metadata returned would be limited to repositories owned by the user the token identifies. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.0.4 and was fixed in versions 3.0.4, 2.22.10, 2.21.18. This vulnerability was reported via the GitHub Bug Bounty program.

CVE-2021-22865 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 **< 3.0.4**

Affected Vendor/Software: **GitHub** - **GitHub Enterprise Server** version **< 2.22.10**

Affected Vendor/Software: **GitHub** - **GitHub Enterprise Server** version **< 2.21.18**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	MEDIUM	NONE
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#3.0.4
Release notes - GitHub Docs	docs.github.com text/html	MISC docs.github.com/en/enterprise-server@2.22/admin/release-notes#2.22.10
Release notes - GitHub Docs	docs.github.com text/html	MISC docs.github.com/en/enterprise-server@2.21/admin/release-notes#2.21.18

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:*:*:*:*:*:*:*:*:

Discovery Credit

djcruz93

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-22865 : An improper access control vulnerability was identified in GitHub Enterprise Server that allowed a… twitter.com/i/web/status/1…	2021-04-02 17:31:36
@3XS0	CVE-2021-22865 An improper access control vulnerability was identified in GitHub Enterprise Server that allowed acc… twitter.com/i/web/status/1…	2021-04-03 00:45:28

← Previous ID

Next ID→

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