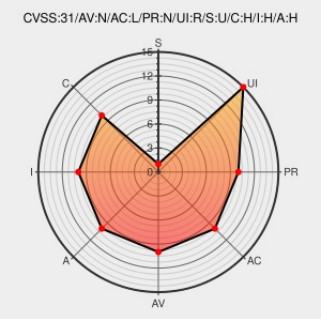
CVE-2021-22866

Published on: 05/14/2021 12:00:00 AM UTC

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

CVE-2021-22866

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



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

A UI misrepresentation vulnerability was identified in GitHub Enterprise Server that allowed more permissions to be granted during a GitHub App's user-authorization web flow than was displayed to the user during approval. 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. All permissions being granted would properly be shown during the first authorization, but in certain circumstances, if the user revisits the authorization flow after the GitHub App has configured additional user-level permissions, those additional permissions may not be shown, leading to more permissions being granted than the user potentially intended. This vulnerability affected GitHub Enterprise Server 3.0.x prior to 3.0.7 and 2.22.x prior to 2.22.13. It was fixed in versions 3.0.7 and 2.22.13. This vulnerability was reported via the GitHub Bug Bounty program.

CVE-2021-22866 has been assigned by product-cna@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **GitHub** - **GitHub Enterprise Server** version **< 3.0.7**

Affected Vendor/Software: **GitHub** - **GitHub Enterprise Server** version **< 2.22.13**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	MEDIUM	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@2.22/admin/release-notes#2.22.13
Release notes - GitHub Docs	docs.github.com text/html	MISC docs.github.com/en/enterprise-server@3.0/admin/release-notes#3.0.7

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

Vaibhav Singh (vaib25vicky)

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-22866 : A UI misrepresentation vulnerability was identified in GitHub Enterprise Server that allowed more… twitter.com/i/web/status/1…	2021-05-14 21:12:57
/r/netcve	CVE-2021-22866	2021-05-14 21:41:39

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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