



CVE-2021-22863

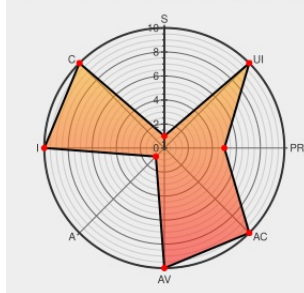
Published on: 03/02/2021 12:00:00 AM UTC

Last Modified on: 10/25/2022 02:03:00 PM UTC

CVE-2021-22863

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N



Certain versions of [Github](#) from [Github](#) contain the following vulnerability:

An improper access control vulnerability was identified in the GitHub Enterprise Server GraphQL API that allowed authenticated users of the instance to modify the maintainer collaboration permission of a pull request without proper authorization. By exploiting this vulnerability, an attacker would be able to gain access to head branches of pull

requests opened on repositories of which they are a maintainer. Forking is disabled by default for organization owned private repositories and would prevent this vulnerability. Additionally, branch protections such as required pull request reviews or status checks would prevent unauthorized commits from being merged without further review or validation. This vulnerability affected all versions of GitHub Enterprise Server since 2.12.22 and was fixed in versions 2.20.24, 2.21.15, 2.22.7 and 3.0.1. This vulnerability was reported via the GitHub Bug Bounty program.

CVE-2021-22863 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 < 2.20.24

Affected Vendor/Software: [GitHub](#) - **GitHub Enterprise Server** version < 2.21.15

Affected Vendor/Software: [GitHub](#) - **GitHub Enterprise Server** version < 2.22.7

Affected Vendor/Software: [GitHub](#) - **GitHub Enterprise Server** version < 3.0.1

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
Release notes - GitHub Docs	Release Notes Vendor Advisory docs.github.com text/html	 MISC docs.github.com/en/enterprise-server@2.21/admin/release-notes#2.21.15
Release notes - GitHub Docs	Release Notes Vendor Advisory docs.github.com text/html	 MISC docs.github.com/en/enterprise-server@3.0/admin/release-notes#3.0.1
Release notes - GitHub Docs	Release Notes Vendor Advisory docs.github.com text/html	 MISC docs.github.com/en/enterprise-server@2.20/admin/release-notes#2.20.24
Release notes - GitHub Docs	Release Notes Vendor Advisory docs.github.com text/html	 MISC docs.github.com/en/enterprise-server@2.22/admin/release-notes#2.22.7

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	All	All	All	All
Application	Github	Github	All	All	All	All
Application	Github	Github	All	All	All	All
Application	Github	Github	All	All	All	All
cpe:2.3:a:github:github:*****:						
cpe:2.3:a:github:github:*****:enterprise:*****:						
cpe:2.3:a:github:github:*****:						
cpe:2.3:a:github:github:*****:enterprise:*****:						

Discovery Credit

Teddy Katz

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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