

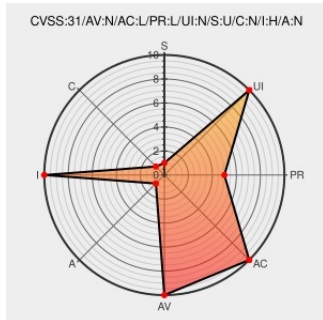


CVE-2022-46258

Published on: Not Yet Published

Last Modified on: 01/30/2023 10:22:12 PM UTC

CVE-2022-46258

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

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

An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed a repository-scoped token with read/write access to modify Action Workflow files without a Workflow scope. The Create or Update file contents API should enforce workflow scope. This vulnerability affected all versions of GitHub Enterprise Server prior to version 3.7 and was fixed in versions 3.3.16, 3.4.11, 3.5.8, and 3.6.4. This vulnerability was reported via the GitHub Bug Bounty program.

CVE-2022-46258 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 < 3.3.16

Affected Vendor/Software: [GitHub](#) - **GitHub Enterprise Server** version < 3.4.11

Affected Vendor/Software: [GitHub](#) - **GitHub Enterprise Server** version < 3.5.8

Affected Vendor/Software: [GitHub](#) - **GitHub Enterprise Server** version < 3.6.4

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	NONE	HIGH	NONE

CVE References

Description	Tags	Link
Release notes - GitHub Enterprise Server 3.5 Docs	docs.github.com text/html	MISC docs.github.com/en/enterprise-server@3.5/admin/release-notes#3.5.8

Release notes - GitHub Enterprise Server 3.6 Docs	docs.github.com text/html	 MISC docs.github.com/en/enterprise-server@3.6/admin/release-notes#3.6.4
Release notes - GitHub Enterprise Server 3.3 Docs	docs.github.com text/html	 MISC docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.16
Release notes - GitHub Enterprise Server 3.4 Docs	docs.github.com text/html	 MISC docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.11

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:*.*.*.*.*.*.*.*.*.*						

Discovery Credit

Alex Ilgayev

Vaibhav Singh (@vaib25vicky)

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-46258 : An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed a... twitter.com/i/web/status/1...	2023-01-09 16:35:01
 /r/netcve	CVE-2022-46258	2023-01-09 17:38:46

[← 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