

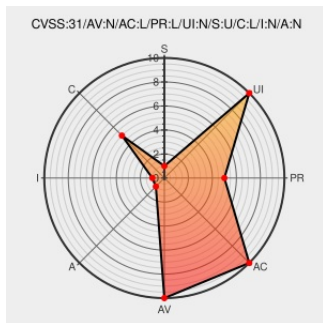


CVE-2020-10517

Published on: 08/27/2020 12:00:00 AM UTC

Last Modified on: 10/07/2021 05:07:00 PM UTC

CVE-2020-10517

[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 authenticated users of the instance to determine the names of unauthorized private repositories given their numerical IDs. This vulnerability did not allow unauthorized access to any repository content besides the name. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22 and was fixed in versions 2.21.6, 2.20.15, and 2.19.21. This vulnerability was reported via the GitHub Bug Bounty program.

CVE-2020-10517 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 < 2.21.6

Affected Vendor/Software: **GitHub - GitHub Enterprise Server** version < 2.20.15

Affected Vendor/Software: **GitHub - GitHub Enterprise Server** version < 2.19.21

CVSS3 Score: **4.3 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
GitHub Enterprise - The best way to build and ship software	Release Notes Vendor Advisory enterprise.github.com text/html	 CONFIRM N/A
GitHub Enterprise - The best way to build and ship software	Release Notes Vendor Advisory enterprise.github.com text/html	 MISC enterprise.github.com/releases/2.19.21/notes
GitHub Enterprise - The best way to build and ship software	Release Notes Vendor Advisory enterprise.github.com text/html	 CONFIRM N/A

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
cpe:2.3:a:github:github:*:*:*:enterprise:*:*:						
cpe:2.3:a:github:github:*:*:*:enterprise:*:*:						

Discovery Credit

William Bowling

Social Mentions

Source	Title	Posted (UTC)
 @4ng3n01r3	#CyberSecurity #Security #CERT #CVE #Nist #Analysed #breach #vulnerability : CVE-2020-10517 (github)	2021-10-07 20:07:04

[← Previous ID](#)[Next ID →](#)

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](#)