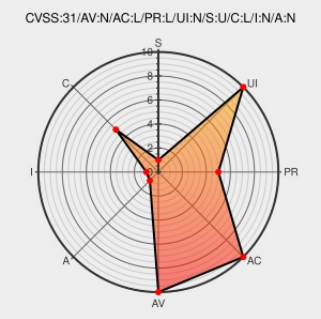
CVE-2021-22868

Published on: 09/24/2021 12:00:00 AM UTC

Last Modified on: 10/01/2021 02:19:00 AM UTC

CVE-2021-22868

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



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

A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.8 and was fixed in 3.1.8, 3.0.16, and 2.22.22. This vulnerability was reported via the GitHub Bug Bounty program. This is the result of an incomplete fix for CVE-2021-22867.

CVE-2021-22868 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 **< 2.22.22**

Affected Vendor/Software: **GitHub** - **GitHub Enterprise Server** version **< 3.0.16**

Affected Vendor/Software: **GitHub** - **GitHub Enterprise Server** version **< 3.1.8**

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
PARTIAL	NONE	NONE

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#2.22.22
Release notes - GitHub Docs	docs.github.com text/html	MISC docs.github.com/en/enterprise-server@3.1/admin/release-notes#3.1.8
Release notes - GitHub Docs	docs.github.com text/html	MISC docs.github.com/en/enterprise-server@3.0/admin/release-notes#3.0.16

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

yvvdwf

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-22868 : A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited… twitter.com/i/web/status/1…	2021-09-24 18:02:13
@SecRiskRptSME	RT: CVE-2021-22868 A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploit… twitter.com/i/web/status/1…	2021-09-25 07:33:21
@threatmeter	CVE-2021-22868 A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited wh… twitter.com/i/web/status/1…	2021-09-25 09:09:51

← Previous ID

Next ID→

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