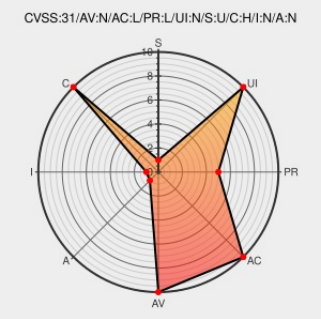
CVE-2023-22380

Published on: Not Yet Published

Last Modified on: 02/27/2023 03:24:00 PM UTC

CVE-2023-22380

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 allowed arbitrary file reading when building a GitHub Pages site. 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 since 3.7 and was fixed in version 3.7.6. This vulnerability was reported via the GitHub Bug Bounty program.

CVE-2023-22380 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 **< 3.7.6**

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	HIGH	NONE	NONE

CVE References

Description	Tags	Link
Release notes - GitHub Enterprise Server 3.7 Docs	docs.github.com text/html	MISC docs.github.com/en/enterprise-server@3.7/admin/release-notes#3.7.6

Related QID Numbers

378566 GitHub Enterprise Server Path Traversal Vulnerability

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-2023-22380 : A path traversal vulnerability was identified in GitHub Enterprise Server that allowed arbitrary f… twitter.com/i/web/status/1…	2023-02-16 20:56:16

← Previous ID

Next ID→