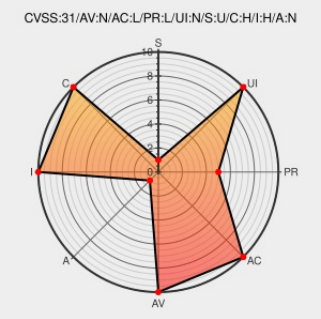
CVE-2023-25559

Published on: Not Yet Published

Last Modified on: 02/21/2023 08:00:00 PM UTC

CVE-2023-25559 - advisory for GHSA-qgp2-qr66-j8r8

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



Certain versions of Datahub from Datahub Project contain the following vulnerability:

DataHub is an open-source metadata platform. When not using authentication for the metadata service, which is the default configuration, the Metadata service (GMS) will use the X-DataHub-Actor HTTP header to infer the user the frontend is sending the request on behalf of. When the backends retrieves the header, its name is retrieved in a case-insensitive way. This case differential can be abused by an attacker to smuggle an X-DataHub-Actor header with different casing (eg: X-DATAHUB-ACTOR). This issue may lead to an authorization bypass by allowing any user to impersonate the system user account and perform any actions on its behalf. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-079.

CVE-2023-25559 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **datahub-project** - **datahub** version **= < 0.8.45**

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

CVE References

Description	Tags	Link
System account impersonation (`GHSL-2022-079`) · Advisory · datahub-project/datahub · GitHub	github.com text/html	MISC github.com/datahub-project/datahub/security/advisories/GHSA-qgp2-qr66-j8r8

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	Datahub Project	Datahub	All	All	All	All

cpe:2.3:a:datahub_project:datahub:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-25559 : DataHub is an open-source metadata platform. When not using authentication for the metadata servic… twitter.com/i/web/status/1…	2023-02-10 23:08:42
/r/netcve	CVE-2023-25559	2023-02-11 00:38:47

← Previous ID

Next ID→

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