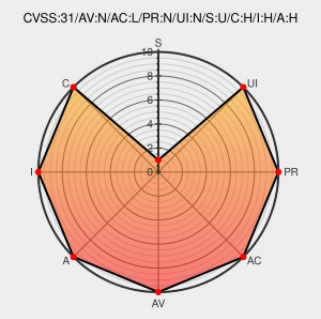
CVE-2023-25560

Published on: Not Yet Published

Last Modified on: 02/21/2023 08:14:00 PM UTC

CVE-2023-25560 - advisory for GHSA-6rpf-5cfg-h8f3

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. The AuthServiceClient which is responsible for creation of new accounts, verifying credentials, resetting them or requesting access tokens, crafts multiple JSON strings using format strings with user-controlled data. This means that an attacker may be able to augment these JSON strings to be sent to the backend and that can potentially be abused by including new or colliding values. This issue may lead to an authentication bypass and the creation of system accounts, which effectively can lead to full system compromise. Users are advised to upgrade. There are no known workarounds for this vulnerability. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-080.

CVE-2023-25560 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

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

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
JSON Injection (`GHSL-2022-080`) · Advisory · datahub-project/datahub · GitHub	github.com text/html	MISC github.com/datahub-project/datahub/security/advisories/GHSA-6rpf-5cfg-h8f3

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)
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-25560 DataHub is an open-source metadata platform. The AuthServiceClien… twitter.com/i/web/status/1…	2023-02-10 22:55:56
@CVEreport	CVE-2023-25560 : DataHub is an open-source metadata platform. The AuthServiceClient which is responsible for creati… twitter.com/i/web/status/1…	2023-02-10 23:09:12
/r/netcve	CVE-2023-25560	2023-02-11 00:38:48

← Previous ID

Next ID→