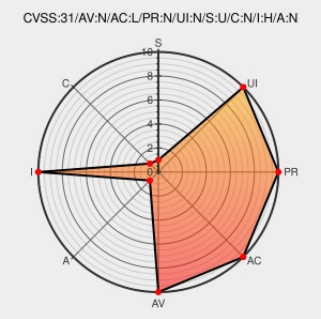
CVE-2023-25570

Published on: Not Yet Published

Last Modified on: 03/01/2023 04:11:00 PM UTC

CVE-2023-25570 - advisory for GHSA-368x-wmmg-hq5c

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



Certain versions of Apollo from Apolloconfig contain the following vulnerability:

Apollo is a configuration management system. Prior to version 2.1.0, there are potential security issues if users expose apollo-configservice to the internet, which is not recommended. This is because there is no authentication feature enabled for the built-in eureka service. Malicious hackers may access eureka directly to mock apollo-configservice and apollo-adminservice. Login authentication for eureka was added in version 2.1.0. As a workaround, avoid exposing apollo-configservice to the internet.

CVE-2023-25570 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **apolloconfig** - **apollo** version **= < 2.1.0**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Enable login authentication for eureka · apolloconfig/apollo@7df79bf · GitHub	github.com text/html	MISC github.com/apolloconfig/apollo/commit/7df79bf8df6960433ed4ff782a54e3dfc74632bd
Potential access control security issue in eureka · Advisory · apolloconfig/apollo · GitHub	github.com text/html	MISC github.com/apolloconfig/apollo/security/advisories/GHSA-368x-wmmg-hq5c
Release Apollo 2.1.0 Release · apolloconfig/apollo · GitHub	github.com text/html	MISC github.com/apolloconfig/apollo/releases/tag/v2.1.0

Enable login authentication for eureka by nobodyiam · Pull Request #4663 · apolloconfig/apollo · GitHub	github.com text/html	MISC github.com/apolloconfig/apollo/pull/4663

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	Apolloconfig	Apollo	All	All	All	All

cpe:2.3:a:apolloconfig:apollo:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-25570 : Apollo is a configuration management system. Prior to version 2.1.0, there are potential security… twitter.com/i/web/status/1…	2023-02-20 16:02:51
/r/netcve	CVE-2023-25570	2023-02-20 17:38:07

← Previous ID

Next ID→