



# CVE-2022-23470

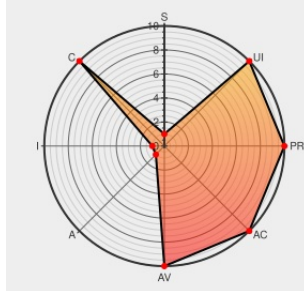
Published on: Not Yet Published

Last Modified on: 12/08/2022 06:00:00 PM UTC

## CVE-2022-23470 - advisory for GHSA-grjf-2ghx-q77x

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Galaxy](#) from [Galaxyproject](#) contain the following vulnerability:

Galaxy is an open-source platform for data analysis. An arbitrary file read exists in Galaxy 22.01 and Galaxy 22.05 due to the switch to Unicorn, which can be used to read any file accessible to the operating system user under which Galaxy is running. This vulnerability affects Galaxy 22.01 and higher, after the switch to unicorn, which serve static contents directly. Additionally, the vulnerability is mitigated when using Nginx or Apache to serve /static/\* contents, instead of Galaxy's internal middleware. This issue has been patched in commit `e5e6bda4f` and will be included in future releases. Users are advised to manually patch their installations. There are no known workarounds for this vulnerability.

CVE-2022-23470 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [galaxyproject](#) - galaxy version = >= 22.01, <= 22.05

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |

### CVE References

| Description                                                                                               | Tags                                                    | Link                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Contain directory traversal for static files to host static root. · galaxyproject/galaxy@e5e6bda · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC</a><br><a href="#">github.com/galaxyproject/galaxy/commit/e5e6bda4f014f807ca77ee0cf6af777a55918346</a> |

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](mailto: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                               | <a href="#">Galaxyproject</a> | <a href="#">Galaxy</a> | All     | All    | All     | All      |
| cpe:2.3:a:galaxyproject:galaxy:*:*:*:*:*: |                               |                        |         |        |         |          |

No vendor comments have been submitted for this CVE

| Social Mentions                                                                               |                                                                                                                                                                      |                     |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Source                                                                                        | Title                                                                                                                                                                | Posted (UTC)        |
|  @CVEreport | CVE-2022-23470 : Galaxy is an open-source platform for data analysis. An arbitrary file read exists in Galaxy 22.01... <a href="#">twitter.com/i/web/status/1...</a> | 2022-12-06 18:03:20 |
|  /r/netcve  | <a href="#">CVE-2022-23470</a>                                                                                                                                       | 2022-12-06 18:55:11 |