



CVE-2023-0994

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-0994 |
| State | PUBLIC |
| Assigner | security@huntr.dev |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-02-24 02:15:00 UTC |
| Updated | 2023-04-26 16:15:00 UTC |
| Description | Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository francoisjacquet/rosariosis prior to 10.8.2. |

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|------------|------------|---------|--------|---------|----------|
| Application | Rosariosis | Rosariosis | All | All | All | All |

References

| Reference | Source | Link |
|---|---------|----------------------------|
| PHP<7 Fix add microseconds to filename to make it harder to predict · francoisjacquet/rosariosis@630d3e3 · GitHub | MISC | github.co |
| huntr – Security Bounties for any GitHub repository | CONFIRM | huntr.dev |
| CVE Program record | CVE.ORG | www.cve |
| NVD vulnerability detail | NVD | nvd.nist.g |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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