



# CVE-2023-2881

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2023-2881   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | security@huntr.dev  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2023-05-25 09:15:00 UTC   |
| <b>Updated</b>         | 2023-05-31 19:21:00 UTC   |
| <b>Description</b>     | Storing Passwords in a Recoverable Format in GitHub repository pimcore/customer-data-framework prior to 3.3.10. |

## Risk And Classification

**Problem Types:** CWE-522

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor  | Product                 | Version | Update | Edition | Language |
|-------------|---------|-------------------------|---------|--------|---------|----------|
| Application | Pimcore | Customer-data-framework | All     | All    | All     | All      |

## References

| Reference   | Source  | Link  | Tags      |
|---|---------|---|-----------|
| huntr – Security Bounties for any GitHub repository   | CONFIRM | <a href="https://huntr.dev">huntr.dev</a>       |           |
| Remove password field from details view (#469) · pimcore/customer-data-framework@d1d58c1 · GitHub | MISC    | <a href="https://github.com">github.com</a>     |           |
| CVE Program record  | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>   | canonical |
| NVD vulnerability detail  | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a> | canonical |

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)