



# CVE-2023-42817

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

## Summary

<b>CVE</b>	CVE-2023-42817
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-25 19:15:00 UTC
<b>Updated</b>	2023-09-26 15:57:00 UTC
<b>Description</b>	Pimcore admin-ui-classic-bundle provides a Backend UI for Pimcore. The translation value with text including "%s" (from "%s")

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pimcore	Admin Classic Bundle	All	All	All	All

## References

Reference	Source
[Bug]: Fix avoid recursion on replaced arguments having further % (#264) · pimcore/admin-ui-classic-bundle@abd7739 · GitHub	MISC
Cross-site Scripting (XSS) in Translations · Advisory · pimcore/admin-ui-classic-bundle · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

995397 PHP (Composer) Security Update for pimcore/admin-ui-classic-bundle (GHSA-m988-7375-7g2c)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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)