



# CVE-2023-49926

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2023-49926                               |
| <b>State</b>           | PUBLISHED                                    |
| <b>Assigner</b>        | Unknown                                      |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback |
| <b>Published</b>       | 2023-12-03 03:15:00 UTC                      |
| <b>Updated</b>         | 2023-12-06 20:51:00 UTC                      |
| <b>Description</b>     | Description unavailable.                     |

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

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

## References

| Reference  | Source  | Link  | Tags      |
|--|---------|---|-----------|
| Comparing v2.4.178...v2.4.179 · MISP/MISP · GitHub   |         | <a href="https://github.com">github.com</a>     | Patch     |
| security: [event:event-timeline] Fixed XSS in the event timeline widget · MISP/MISP@dc73287 · GitHub |         | <a href="https://github.com">github.com</a>     | Patch     |
| 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)