



# CVE-2022-34529

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2022-34529   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2022-07-27 14:15:00 UTC  |
| <b>Updated</b>         | 2023-08-08 14:21:00 UTC  |
| <b>Description</b>     | WASM3 v0.5.0 was discovered to contain a segmentation fault via the component Compile_Memory_CopyFill. |

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor        | Product | Version | Update | Edition | Language |
|-------------|---------------|---------|---------|--------|---------|----------|
| Application | Wasm3 Project | Wasm3   | 0.5.0   | All    | All     | All      |

## References

| Reference   | Source  | Link                   |
|---|---------|------------------------|
| [Segmentation fault] slot index overflow because of slot missing in some bytecode · Issue #337 · wasm3/wasm3 · GitHub | MISC    | <a href="#">github</a> |
| CVE Program record  | CVE.ORG | <a href="#">www</a>    |
| NVD vulnerability detail  | NVD     | <a href="#">nvd.n</a>  |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

994916 Python (Pip) Security Update for pywasm3 (GHSA-gq4p-4hvx-5rg9)

994918 Rust (Rust) Security Update for wasm3 (GHSA-gq4p-4hvx-5rg9)

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)