

CVE-2025-48044

Authorization bypass when bypass policy condition evaluates to true

[« Back to all CVEs](#)[See on OSV.dev »](#)

Weakness Type (CWE)

[CWE-863 — CWE-863 Incorrect Authorization](#)

CAPEC

[CAPEC-115 — CAPEC-115 Authentication Bypass](#)

CVSS 4.0 Score

8.6

HIGH

[CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N](#)

Vulnerability description

Incorrect Authorization vulnerability in ash-project ash allows Authentication Bypass.

This vulnerability is associated with program files `lib/ash/policy/policy.ex` and program routines `'Elixir.Ash.Policy.Policy':expression/2`.

This issue affects ash: from `pkg:hex/ash@3.6.3` before `pkg:hex/ash@3.7.1`, from 3.6.3 before 3.7.1, from `79749c2685ea031ebb2de8cf60cc5edced6a8dd0` before [→ 8b83efa225](#).

Affected

[pkg:hex/ash](#)

Source File

[lib/ash/policy/policy.ex](#)

Routine

[Ash.Policy.Policy.expression/2](#)

Status

Affected

Type

semver [①](#)

Version

[3.6.3](#)

Changes / Fixed in

< [3.7.1](#)[pkg:github/ash-project/ash](#)

Source File

[lib/ash/policy/policy.ex](#)

Routine

Ash.Policy.Policy.expression/2

Status

Affected

Type

git [①](#)

Version

[79749c2685](#)

Changes / Fixed in

< [8b83efa225](#)

References

- <https://github.com/ash-project/ash/security/advisories/GHSA-pcxq-fjp3-r752> vendor-advisory related
- <https://osv.dev/vulnerability/EEF-CVE-2025-48044> related
- <https://github.com/ash-project/ash/commit/8b83efa225f657bfc3656ad8ee8485f9b2de923d> patch

Credits

- **Reporter:** Jechol Lee
- **Remediation developer:** Jechol Lee
- **Analyst:** Jonatan Männchen
- **Remediation reviewer:** Zach Daniel

CVE record as JSON: [GET /cves/CVE-2025-48044.json](#)

OSV record as JSON: [GET /osv/EEF-CVE-2025-48044.json](#)



ERLANG ECOSYSTEM
FOUNDATION

Supporting the BEAM community

ABOUT THE EEF

[Membership details](#)

[Join us!](#)

[Sponsors](#)

[Working Groups](#)

[Stipends](#)

[Bylaws](#)

[FAQ](#)

STAY UP-TO-DATE

[News](#)

[Events](#)

GET IN TOUCH

[Contact Us](#)

