EEF-CVE-2025-48044

See a problem?
Please try reporting it to the source first.

Source	https://cna.erlef.org/osv/EEF-CVE-2025-48044.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2025-48044.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2025-48044
Aliases	CVE-2025-48044 GHSA-pcxq-fjp3-r752
Published	2025-10-17T13:52:53.644Z
Modified	2026-04-06T17:01:50.482632Z
Severity	8.6 (High) CVSS_V4 - 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 CVSS Calculator
Summary	Authorization bypass when bypass policy condition evaluates to true
Details	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 8b83efa225f657bfc3656ad8ee8485f9b2de923d.

Database specific


```
{
    "cwe_ids": [
        "CWE-863"
    ],
    "cpe_ids": [
        "cpe:2.3:a:ash-project:ash:*:*:*:*:*:*:*:*"
    ],
    "capec_ids": [
        "CAPEC-115"
```

```
      ]
}
```

References

https://github.com/ash-project/ash/security/advisories/GHSA-pcxq-fjp3-r752

https://cna.erlef.org/cves/CVE-2025-48044.html

https://github.com/ash-project/ash/commit/8b83efa225f657bfc3656ad8ee8485f9b2de923d

https://hex.pm/packages/ash

Credits

Jechol Lee - REPORTER

Jechol Lee - REMEDIATION_DEVELOPER

Jonatan Männchen - ANALYST

Zach Daniel - REMEDIATION_REVIEWER

Affected packages

Hex
ash

Git
github.com/ash-project/ash

Package

Name ash

Purl pkg:hex/ash

Affected ranges

Type SEMVER

Events Introduced
3.6.3
Fixed
3.7.1

Affected versions

▸ 3.*

Database specific

▸ source