



# Missing Session Revocation on Logout in ash\_authentication\_phoenix

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

## Summary

<b>CVE</b>	CVE-2025-4754
<b>State</b>	PUBLISHED
<b>Assigner</b>	EEF
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-06-17 15:15:53 UTC
<b>Updated</b>	2026-04-06 17:17:04 UTC

**Description** Insufficient Session Expiration vulnerability in ash-project ash\_authentication\_phoenix allows Session Hijacking. This vulner

## Risk And Classification

**Primary CVSS:** v4.0 2.3 LOW from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-613 | CWE-613 CWE-613 Insufficient Session Expiration

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	2.3	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N
4.0	CNA	CVSS	2.3	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Ash-project</a>	<a href="#">Ash Authentication Phoenix</a>	affected 2.10.0 semver	Not specified
CNA	<a href="#">Ash-project</a>	<a href="#">Ash Authentication Phoenix</a>	affected a3253fb4fc7145aeb403537af1c24d3a8d51ffb1 git	Not specified

### References

Reference	Source	Link
<a href="https://github.com/team-alembic/ash_authentication_phoenix/security/advisories/G...">github.com/team-alembic/ash_authentication_phoenix/security/advisories/G...</a>	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="#">github.com</a>
<a href="https://osv.dev/vulnerability/EEF-CVE-2025-4754">osv.dev/vulnerability/EEF-CVE-2025-4754</a>	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="#">osv.dev</a>
<a href="https://github.com/team-alembic/ash_authentication_phoenix/pull/634">github.com/team-alembic/ash_authentication_phoenix/pull/634</a>	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="#">github.com</a>
<a href="https://github.com/team-alembic/ash_authentication_phoenix/commit/a3253fb4fc7145...">github.com/team-alembic/ash_authentication_phoenix/commit/a3253fb4fc7145...</a>	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="#">github.com</a>
<a href="https://cna.erlef.org/cves/CVE-2025-4754.html">cna.erlef.org/cves/CVE-2025-4754.html</a>	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="#">cna.erlef.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** James Harton (en)

**CNA:** Zach Daniel (en)

**CNA:** Mike Buhot (en)

**CNA:** Jonatan Männchen (en)

**CNA:** Josh Price (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)