



Authorization bypass when bypass policy condition evaluates to true

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

Summary

CVE	CVE-2025-48044
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-17 14:15:46 UTC
Updated	2026-04-06 17:17:04 UTC
Description	Incorrect Authorization vulnerability in ash-project ash allows Authentication Bypass. This vulnerability is associated with pr

Risk And Classification

Primary CVSS: v4.0 8.6 HIGH from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

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/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-863 | CWE-863 CWE-863 Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	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/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
4.0	CNA	CVSS	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/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

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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/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
CNA	Ash-project	Ash	affected 3.6.3 3.7.1 semver
CNA	Ash-project	Ash	affected 79749c2685ea031ebb2de8cf60cc5edced6a8dd0 8b83efa225f657bfc3656ad8ee8485f9b2de923d

References

Reference	Source	Link
github.com/ash-project/ash/security/advisories/GHSA-pcxq-fjp3-r752	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
cna.erlef.org/cves/CVE-2025-48044.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.org
github.com/ash-project/ash/commit/8b83efa225f657bfc3656ad8ee8485f9b2de923d	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
osv.dev/vulnerability/EEF-CVE-2025-48044	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Jechol Lee (en)

CNA: Jechol Lee (en)

CNA: Jonatan Männchen (en)

CNA: Zach Daniel (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](#)