



# Keycloak: org.keycloak.protocol.oidc.grants.ciba: keycloak: information disclosure via cors header injection due to unvalidated jwt azp claim

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

## Summary

<b>CVE</b>	CVE-2026-37977
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-06 09:16:17 UTC
<b>Updated</b>	2026-04-07 13:20:35 UTC
<b>Description</b>	A flaw was found in Keycloak. A remote attacker can exploit a Cross-Origin Resource Sharing (CORS) header injection vul

## Risk And Classification

**Primary CVSS:** v3.1 3.7 LOW from secalert@redhat.com

**CVSS:** 3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

**EPSS:** 0.000070000 probability, percentile 0.005270000 (date 2026-04-07)

**Problem Types:** CWE-346 | CWE-346 Origin Validation Error

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Keycloak	Not specified	Not specified

### References

Reference	Source	Link	Tags
<a href="https://access.redhat.com/security/cve/CVE-2026-37977">access.redhat.com/security/cve/CVE-2026-37977</a>	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>	secalert@redhat.com	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

Source	Time	Event
CNA	2026-04-06T07:49:33.467Z	Reported to Red Hat.
CNA	2026-04-06T08:34:01.137Z	Made public.

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](#).

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)