



# Keycloak: org.keycloak/keycloak-services: keycloak: privilege escalation via manage-clients permission

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

## Summary

<b>CVE</b>	CVE-2026-3121
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-26 19:17:06 UTC
<b>Updated</b>	2026-04-01 14:06:42 UTC
<b>Description</b>	A flaw was found in Keycloak. An administrator with `manage-clients` permission can exploit a misconfiguration where this

## Risk And Classification

**Primary CVSS:** v3.1 7.2 HIGH from nvd@nist.gov

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

**EPSS:** 0.000280000 probability, percentile 0.077700000 (date 2026-04-01)

**Problem Types:** CWE-266 | CWE-266 Incorrect Privilege Assignment

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	secalert@redhat.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Build Of Keycloak	-	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	8.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform Expansion Pack	-	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Keycloak	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	Not specified	Not specified
CNA	Red Hat	Red Hat Single Sign-On 7	Not specified	Not specified

### References

Reference	Source	Link	Tags
<a href="https://access.redhat.com/security/cve/CVE-2026-3121">access.redhat.com/security/cve/CVE-2026-3121</a>	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	Vendor Advisory
<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>	Issue Tracking, Vendor Advisory
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	2026-02-24T13:06:55.355Z	Reported to Red Hat.
CNA	2026-02-24T11:11:00.000Z	Made public.

### Workarounds

**CNA:** Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment,

applicability to widespread installation base or stability.

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](#)**