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

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-3121
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 19:17:06 UTC
Updated	2026-04-01 14:06:42 UTC
Description	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

ntegrity

High

vailability

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
access.redhat.com/security/cve/CVE-2026-3121	secalert@redhat.com	access.redhat.com	Vendor Advisory
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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.