



# CVE-2023-6291

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

## Summary

<b>CVE</b>	CVE-2023-6291
<b>State</b>	PUBLISHED
<b>Assigner</b>	Unknown
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-01-26 15:15:00 UTC
<b>Updated</b>	2024-02-04 20:15:00 UTC
<b>Description</b>	Description unavailable.

## Risk And Classification

**Problem Types:** CWE-601

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Keycloak</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Migration Toolkit For Applications</a>	6.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Migration Toolkit For Applications</a>	7.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.11	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.12	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform For Ibm Z</a>	4.10	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform For Ibm Z</a>	4.9	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform For Linuxone</a>	4.10	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform For Linuxone</a>	4.9	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform For Power</a>	4.10	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform For Power</a>	4.9	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Single Sign-on</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Single Sign-on</a>	7.6	All	All	All

## References

REFERENCES

Reference	Source	Link	Tags
Red Hat		<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat		<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat		<a href="https://access.redhat.com">access.redhat.com</a>	
2251407 – (CVE-2023-6291) CVE-2023-6291 keycloak: redirect_uri validation bypass		<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
Red Hat		<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat		<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat		<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat		<a href="https://access.redhat.com">access.redhat.com</a>	
cve-details		<a href="https://access.redhat.com">access.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.

Legacy QID Mappings

996431 Java (Maven) Security Update for org.keycloak:keycloak-services (GHSA-mpwq-j3xf-7m5w)

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). 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)