Org.keycloak.forms.login: keycloak: keycloak: arbitrary code execution via stored cross-site scripting (xss) in organization selection login page

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-37980
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 15:16:34 UTC
Updated	2026-04-17 15:11:03 UTC
Description	A flaw was found in Keycloak, specifically in the organization selection login page. A remote attacker with `manage-realm` c

Risk And Classification

Primary CVSS: v3.1 6.9 MEDIUM from secalert@redhat.com

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

EPSS: 0.000550000 probability, percentile 0.171180000 (date 2026-04-21)

Problem Types: CWE-79 | CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	6.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:L/A:N
3.1	CNA	CVSS	6.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:L/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
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-37980	secalert@redhat.com	access.redhat.com	
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	2026-04-06T07:51:18.531Z	Reported to Red Hat.
CNA	2026-04-06T12:34:00.000Z	Made public.

Workarounds

CNA: Restrict access to the Keycloak administration console and login pages to trusted networks only, ideally through a VPN or by configuring firewall rules. Furthermore, ensure that only highly trusted administrators are granted `manage-realm` or `manage-organizations` privileges within Keycloak. Regularly review and audit administrative accounts and their assigned roles to minimize the risk of unauthorized access and exploitation. If the Keycloak service is restarted or reloaded, these network and access restrictions will persist.

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 registred 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

CVE.report and Source URL Uptime Status status.cve.report