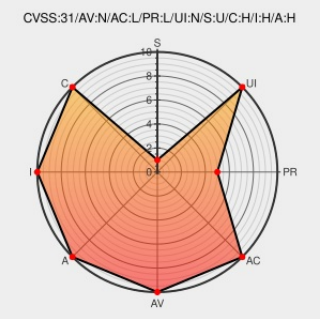
CVE-2021-4133

Published on: Not Yet Published

Last Modified on: 09/03/2022 03:33:00 AM UTC

CVE-2021-4133

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Keycloak from Redhat contain the following vulnerability:

A flaw was found in Keycloak in versions from 12.0.0 and before 15.1.1 which allows an attacker with any existing user account to create new default user accounts via the administrative REST API even when new user registration is disabled.

CVE-2021-4133 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Oracle Critical Patch Update Advisory - April 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpuapr2022.html
2033602 – (CVE-2021-4133) CVE-2021-4133 Keycloak: Incorrect authorization allows unpriviledged users to create	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=2033602

other users

Incorrect authorization allows unpriviledged users to create other users · Issue #9247 · keycloak/keycloak · GitHub	github.com text/html	MISC github.com/keycloak/keycloak/issues/9247
Incorrect authorization allows unpriviledged users to create other users · Advisory · keycloak/keycloak · GitHub	github.com text/html	MISC github.com/keycloak/keycloak/security/advisories/GHSA-83x4-9cwr-5487

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Keycloak	All	All	All	All

cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@scne59	And now for something completely different: access.redhat.com/security/cve/c… #keycloak	2021-12-20 18:49:17
@fpientka	CVE-2021-4133 @keycloak version from 12.0.0 and before 15.1.1 allows an attacker with any existing user account t… twitter.com/i/web/status/1…	2021-12-21 06:54:56
@stymied_sloth	@JLLeitschuh @keycloak CVE-2021-4133	2021-12-21 15:40:16
@cloud_iam_com	#changelog Keycloak v15.1.1 Critical Update. A critical flaw (CVE-2021-4133) was found today in Keycloak version f… twitter.com/i/web/status/1…	2021-12-23 21:17:23
@management_sun	IT Risk: Red Hat.Single Sign-On 7.5.1に複数の脆弱性 -2/2 CVE-2021-4133 CVE-2021-3827	2022-01-18 07:07:46
@CVEreport	CVE-2021-4133 : A flaw was found in Keycloak in versions from 12.0.0 and before 15.1.1 which allows an attacker wit… twitter.com/i/web/status/1…	2022-01-25 20:15:11
/r/netcve	CVE-2021-4133	2022-01-25 21:39:14

← Previous ID

Next ID→

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.

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