



CVE-2021-3513

Published on: Not Yet Published

Last Modified on: 08/23/2022 06:35:00 PM UTC

CVE-2021-3513

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Keycloak](#) from [Redhat](#) contain the following vulnerability:

A flaw was found in keycloak where a brute force attack is possible even when the permanent lockout feature is enabled. This is due to a wrong error message displayed when wrong credentials are entered. The highest threat from this vulnerability is to confidentiality.

CVE-2021-3513 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
1953439 – (CVE-2021-3513) CVE-2021-3513 keycloak: Brute force attack is possible even after the account lockout	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1953439
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2021-3513

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

Exploit/POC from Github

A flaw was found in keycloak where a brute force attack is possible even when the permanent lockout feature is enable...

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)
 @kurtseifried	But a good example of this is CVE-2021-3513 which Red Hat (a CNA) and ArchLinux have shipped updates for referring... twitter.com/i/web/status/1...	2022-06-24 04:28:33
 @CVEreport	CVE-2021-3513 : A flaw was found in keycloak where a brute force attack is possible even when the permanent lockout... twitter.com/i/web/status/1...	2022-08-22 15:15:10
 @threatmeter	CVE-2021-3513 A flaw was found in keycloak where a brute force attack is possible even when the permanent lockout f... twitter.com/i/web/status/1...	2022-08-23 07:09:32
 @ColorTokensInc	Emerging Vulnerability Found CVE-2021-3513 - A flaw was found in keycloak where a brute force attack is possible ev... twitter.com/i/web/status/1...	2022-08-23 18:42:17
 @LinInfoSec	Keycloak - CVE-2021-3513: bugzilla.redhat.com/show_bug.cgi?i...	2022-08-23 22:03:02
 /r/netcve	CVE-2021-3513	2022-08-22 15:38:35

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)