CVE-2017-12161

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

Summary

CVE	CVE-2017-12161
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-21 18:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	It was found that keycloak before 3.4.2 final would permit misuse of a client-side /etc/hosts entry to spoof a URL in a passw

Risk And Classification

Problem Types: CWE-640

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
1484564 – (CVE-2017-12161) CVE-2017-12161 keycloak: reset password token disclosure
KEYCLOAK-5299 Document how to explicitly set permitted hostnames by stianst · Pull Request #268 · keycloak/keycloak-documentation · Git
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

983152 Java (maven) Security Update for org.keycloak:keycloak-core (GHSA-959q-32g8-vvp7)

© 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