

# SSO - Keycloak

JF Perrin

- Single Sign On
  - Life is simpler for your users, login once.
- No more password exchange between users and applications.
  - Clear security improvement for the organisation
  - Single point where you can strengthen security measures (fail2ban like, 2FA, ...).

# Keycloak why?

---

- Production ready software since several years
- Open Source (easy adoption)
- Very active project
- Multi protocol: OAuth2, SAML
- Different auth flow possible: OTP, WebAuthn, ...
- Comprehensive management interface (Web GUI)
- Allow easily to map identities (bridging)

# Keycloak why?

- Supported by RedHat

## CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#)

[Home](#)

**Browse :**

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

**Reports :**

[CVSS Score Report](#)

[CVSS Score Distribution](#)

**Search :**

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

**Top 50 :**

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

**Other :**

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CVE Definitions](#)

[About & Contact](#)

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

**Vulnerability Feeds & Widgets<sup>New</sup>** [www.itsecdb.com](http://www.itsecdb.com)

### Keycloak : Security Vulnerabilities

CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2017-12160</a>	<a href="#">287</a>			2017-10-26	2019-10-09	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
It was found that Keycloak oauth would permit an authenticated resource to obtain an access/refresh token pair from the authentication server, permitting indefinite usage in the case of permission revocation. An attacker on an already compromised resource could use this flaw to grant himself continued permissions and possibly conduct further attacks.														
2	<a href="#">CVE-2017-12159</a>	<a href="#">613</a>		CSRF	2017-10-26	2019-10-09	5.0	None	Remote	Low	Not required	Partial	None	None
It was found that the cookie used for CSRF prevention in Keycloak was not unique to each session. An attacker could use this flaw to gain access to an authenticated user session, leading to possible information disclosure or further attacks.														
3	<a href="#">CVE-2017-12158</a>	<a href="#">79</a>		XSS	2017-10-26	2019-10-09	3.5	None	Remote	Medium	Single system	None	Partial	None
It was found that Keycloak would accept a HOST header URL in the admin console and use it to determine web resource locations. An attacker could use this flaw against an authenticated user to attain reflected XSS via a malicious server.														
4	<a href="#">CVE-2017-7474</a>			Bypass	2017-05-12	2019-10-02	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
It was found that the Keycloak Node.js adapter 2.5 - 3.0 did not handle invalid tokens correctly. An attacker could use this flaw to bypass authentication and gain access to restricted information, or to possibly conduct further attacks.														
5	<a href="#">CVE-2014-3709</a>	<a href="#">352</a>		CSRF	2017-10-18	2017-11-07	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
The org.keycloak.services.resources.SocialResource.callback method in JBoss KeyCloak before 1.0.3.Final allows remote attackers to conduct cross-site request forgery (CSRF) attacks by leveraging lack of CSRF protection.														

Total number of vulnerabilities : 5 Page : 1 (This Page)

# Keycloak why?



Google

keycloak training

x | 🔍



View all

<https://www.udemy.com/course/keycloak-single-sig...>

## Keycloak : Single Sign On with Spring Boot & Spring Security

In this **course** you will learn **Keycloak** which is an open source software product to allow single sign-on with Identity and Access Management aimed at modern ...

<https://www.janua.fr/keycloak-redhat-sso-openidm-op...>

## KeyCloak Redhat SSO OpenIDM OpenDJ Training - JANUA

Janua offers **KeyCloak** Redhat SSO OpenIDM Open DJ trainings, in French and English, on the main open source identity management products. The **course** ...

<https://training.zenika.com/accueil/keycloak>

## Programme de la formation Keycloak, Zenika

Programme de formation pour Savoir mettre en place et configurer **Keycloak**, Zenika. ... Zenika Training Logo ... Je déploie et configure **Keycloak**.

<https://training.zenika.com/fr-fr/keycloak/description>

## Keycloak - Formations Zenika

Une question ? [training@zenika.com](mailto:training@zenika.com) +33(0)1 45 26 19 15.

<https://www.katacoda.com/sebastienblanc/courses>

## Keycloak course using Interactive Browser-Based Labs

**Keycloak course**. By Sébastien Blanc. A serie of scenarios that will teach you how to setup and use Keycloak. Configure Keycloak. Set up your first Realm, ...

<https://www.ambient-it.net/uploads/2021/05/PDF>

## Training Keycloak - Ambient IT

In this **training**, we'll explore most of the **Keycloak** capabilities and features that help you secure your applications and services. You'll discover how you can ...

- You are free to use an SSO or not
- Keycloak is one solution, other exists
- Keycloak is not part of UmbrellaID scope
  
- In use at ILL, ESRF, ESS ...