umbrella

SSO - Keycloack

JF Perrin

umbrella

SSO Why?

- 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, …).

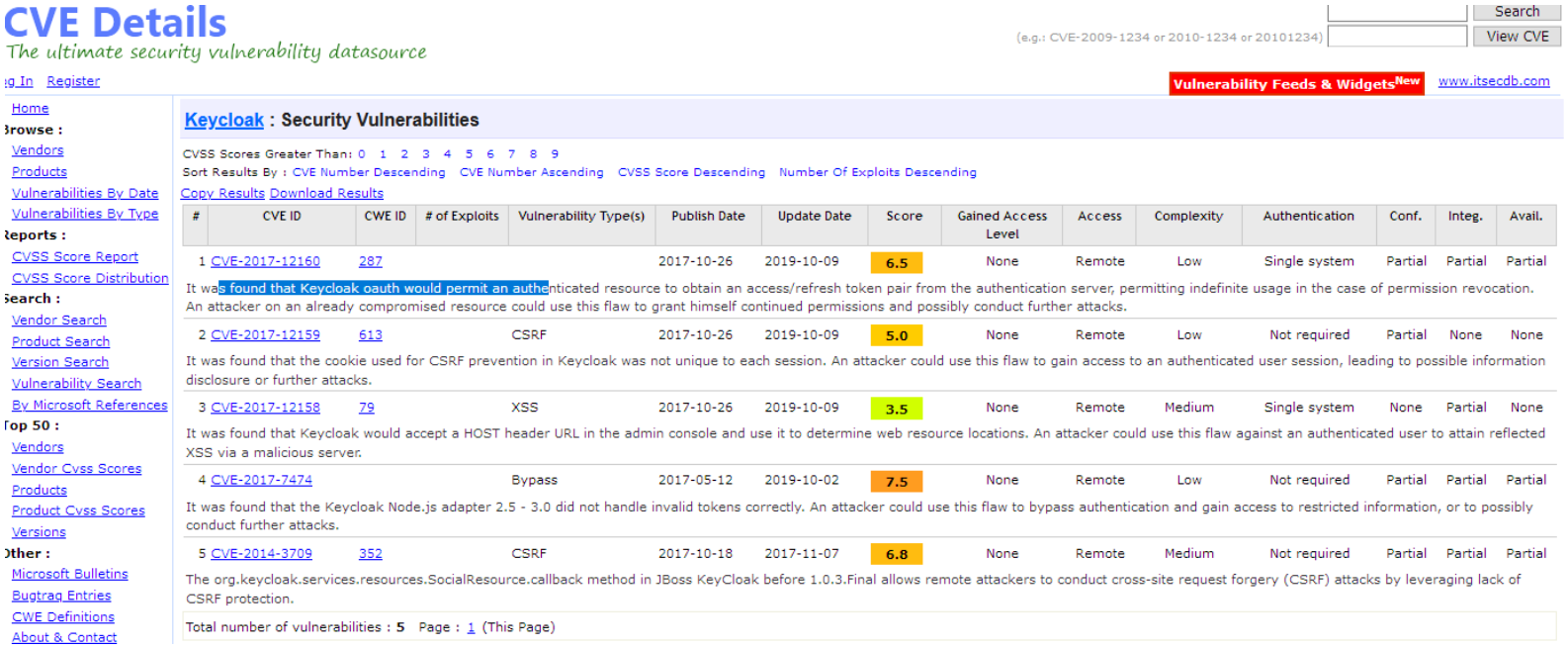
umbrella

Keycloack why?

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

Keycloack why?

- Supported by RedHat



CVE Details
The ultimate security vulnerability datasource

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

g In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

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
CWE Definitions
About & Contact

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	CVE-2017-12160	287			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	CVE-2017-12159	613		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	CVE-2017-12158	79		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	CVE-2017-7474			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	CVE-2014-3709	352		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)

umbrella

- You are free to use an SSO or not
- Keycloak is one solution, other exists

- In use at ILL, ESRF, …