Bug 2312511 (CVE-2024-8883) - CVE-2024-8883 Keycloak: Vulnerable Redirect URI Validation Results in Open Redirec

Keywords: Security ×

Status: NEW

Alias: CVE-2024-8883

Deadline: 2024-09-19

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2024-09-16 06:28 UTC by OSIDB Bzimport

Modified: 2026-04-30 04:01 UTC (History)

CC List: 39 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed: Yes

Attachments (Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2024:10385	0	None	None	None	2024-11-26 15:35:28 UTC
Red Hat Product Errata	RHSA-2024:10386	0	None	None	None	2024-11-26 15:36:04 UTC

Red Hat Product Errata	RHSA-2024:6878	0	None	None	None	2024-09-19 16:41:19 UTC
Red Hat Product Errata	RHSA-2024:6879	0	None	None	None	2024-09-19 16:41:24 UTC
Red Hat Product Errata	RHSA-2024:6880	0	None	None	None	2024-09-19 16:41:36 UTC
Red Hat Product Errata	RHSA-2024:6882	0	None	None	None	2024-09-19 16:45:49 UTC
Red Hat Product Errata	RHSA-2024:6886	0	None	None	None	2024-09-19 16:54:31 UTC
Red Hat Product Errata	RHSA-2024:6887	0	None	None	None	2024-09-19 17:07:04 UTC
Red Hat Product Errata	RHSA-2024:6888	0	None	None	None	2024-09-19 17:02:48 UTC
Red Hat Product Errata	RHSA-2024:6889	0	None	None	None	2024-09-19 17:10:47 UTC
Red Hat Product Errata	RHSA-2024:6890	0	None	None	None	2024-09-19 17:06:41 UTC
Red Hat Product Errata	RHSA-2024:8823	0	None	None	None	2024-11-04 20:12:13 UTC
Red Hat Product Errata	RHSA-2024:8824	0	None	None	None	2024-11-04 20:11:49 UTC
Red Hat Product Errata	RHSA-2024:8826	0	None	None	None	2024-11-04 20:56:40 UTC

OSIDB Bzimport 2024-09-16 06:28:19 UTC Description

```
It is possible to configure Keycloak in such a manner that any
application with a 'Valid Redirect URI' set to
http://localhost or http://127.0.0.1 can be redirected to an
```

arbitrary URL of the attackers choosing. In the process sensitive information such as the authorization code can be exposed to the attacker, resulting in possible session hijacking.

errata-xmlrpc 2024-09-19 16:41:17 UTC Comment 3

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 7

Via RHSA-2024:6878 https://access.redhat.com/errata/RHSA-2024:6878

errata-xmlrpc 2024-09-19 16:41:21 UTC Comment 4

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 8

Via RHSA-2024:6879 https://access.redhat.com/errata/RHSA-2024:6879

errata-xmlrpc 2024-09-19 16:41:34 UTC Comment 5

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 9

Via RHSA-2024:6880 https://access.redhat.com/errata/RHSA-2024:6880

errata-xmlrpc 2024-09-19 16:45:46 UTC Comment 6

This issue has been addressed in the following products:

RHEL-8 based Middleware Containers

Via RHSA-2024:6882 https://access.redhat.com/errata/RHSA-2024:6882

errata-xmlrpc 2024-09-19 16:54:29 UTC Comment 7

This issue has been addressed in the following products:

  Red Hat Single Sign-On

Via RHSA-2024:6886 https://access.redhat.com/errata/RHSA-2024:6886

errata-xmlrpc 2024-09-19 17:02:46 UTC Comment 8

This issue has been addressed in the following products:

  Red Hat build of Keycloak 22

Via RHSA-2024:6888 https://access.redhat.com/errata/RHSA-2024:6888

errata-xmlrpc 2024-09-19 17:06:38 UTC Comment 9

This issue has been addressed in the following products:

  Red Hat build of Keycloak 22

Via RHSA-2024:6890 https://access.redhat.com/errata/RHSA-2024:6890

errata-xmlrpc 2024-09-19 17:07:01 UTC Comment 10

This issue has been addressed in the following products:

  Red Hat build of Keycloak 22

Via RHSA-2024:6887 https://access.redhat.com/errata/RHSA-2024:6887

errata-xmlrpc 2024-09-19 17:10:45 UTC Comment 11

This issue has been addressed in the following products:

  Red Hat build of Keycloak 24

Via RHSA-2024:6889 https://access.redhat.com/errata/RHSA-2024:6889

errata-xmlrpc 2024-11-04 20:11:47 UTC Comment 12

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 9

Via RHSA-2024:8824 https://access.redhat.com/errata/RHSA-2024:8824

errata-xmlrpc 2024-11-04 20:12:10 UTC Comment 13

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 8

Via RHSA-2024:8823 https://access.redhat.com/errata/RHSA-2024:8823

errata-xmlrpc 2024-11-04 20:56:37 UTC Comment 14

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform

Via RHSA-2024:8826 https://access.redhat.com/errata/RHSA-2024:8826

errata-xmlrpc 2024-11-26 15:35:26 UTC Comment 15

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform

Via RHSA-2024:10385 https://access.redhat.com/errata/RHSA-2024:10385

errata-xmlrpc 2024-11-26 15:36:02 UTC Comment 16

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 9
  Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 8

Via RHSA-2024:10386 https://access.redhat.com/errata/RHSA-

2024:10386

Note

You need to log in before you can comment on or make changes to this bug.