Bug 2040268 (CVE-2022-0225) - CVE-2022-0225 keycloak: Stored XSS in groups dropdown

Keywords: Security ×

Status: NEW

Alias: CVE-2022-0225

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks: 🔒 2040242 🔒 2040468

TreeView+ depends on / blocked

Reported: 2022-01-13 10:42 UTC by Paramvir jindal

Modified: 2022-11-03 15:16 UTC (History)

CC List: 7 users (show)

Fixed In Version:

Doc Type: ---

Doc Text:

```
A flaw was found in
Keycloak. This flaw
allows a privileged
attacker to use the
malicious payload as the
group name while creating
a new group from the
admin console, leading to
a stored Cross-site
scripting (XSS) attack.
```

Clone Of:

Environment:

Last Closed:

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2022:6782	0	None	None	None	2022-10-04 15:37:52 UTC
Red Hat Product Errata	RHSA-2022:6783	0	None	None	None	2022-10-04 15:41:44 UTC
Red Hat Product Errata	RHSA-2022:6787	0	None	None	None	2022-10-04 15:53:48 UTC

Red Hat Product Errata	RHSA-2022:7409	0	None	None	None	2022-11-03 14:51:44 UTC
Red Hat Product Errata	RHSA-2022:7410	0	None	None	None	2022-11-03 14:51:23 UTC
Red Hat Product Errata	RHSA-2022:7411	0	None	None	None	2022-11-03 14:52:30 UTC
Red Hat Product Errata	RHSA-2022:7417	0	None	None	None	2022-11-03 15:16:17 UTC

Paramvir jindal 2022-01-13 10:42:11 UTC Description

```
The ”Groups” dropdown in ”Add user” is not escaped properly
and can be exploited.

Steps to reproduce

    Start a vanilla keycloak (or an existing one):
    docker run -p 8080:8080 -e KEYCLOAK_USER=admin -e
KEYCLOAK_PASSWORD=admin quay.io/keycloak/keycloak:16.1.0
    Login and go to Groups.
    Click New to add a new group.
    Add a group using the payload below:

"><img src=x onerror=prompt(location)>

    Go to Users and click Add user.
    Click Groups and enter a character, as o, to display the
group. This will trigger our prompt from the group name.

Maybe also other places has this issue?
This is probably an easy fix for you, but in case you want me
to look into it I can do it. I’m jxn0 on github.
```

Paramvir jindal 2022-01-13 10:43:40 UTC Comment 1

```
I have replicated this issue with latest upstream keycloak
16.0.1 and latest RHSSO i.e. 7.5
```

errata-xmlrpc 2022-10-04 15:37:49 UTC Comment 5

```
This issue has been addressed in the following products:

  Red Hat Single Sign-On 7.5 for RHEL 7

Via RHSA-2022:6782 https://access.redhat.com/errata/RHSA-
```

2022:6782

errata-xmlrpc 2022-10-04 15:41:42 UTC Comment 6

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.5 for RHEL 8

Via RHSA-2022:6783 https://access.redhat.com/errata/RHSA-2022:6783

errata-xmlrpc 2022-10-04 15:53:45 UTC Comment 7

This issue has been addressed in the following products:

Red Hat Single Sign-On

Via RHSA-2022:6787 https://access.redhat.com/errata/RHSA-2022:6787

errata-xmlrpc 2022-11-03 14:51:22 UTC Comment 9

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 8

Via RHSA-2022:7410 https://access.redhat.com/errata/RHSA-2022:7410

errata-xmlrpc 2022-11-03 14:51:42 UTC Comment 10

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 7

Via RHSA-2022:7409 https://access.redhat.com/errata/RHSA-2022:7409

errata-xmlrpc 2022-11-03 14:52:29 UTC Comment 11

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 9

Via RHSA-2022:7411 https://access.redhat.com/errata/RHSA-2022:7411 errata-xmlrpc 2022-11-03 15:16:06 UTC Comment 12

This issue has been addressed in the following products:

  Red Hat Single Sign-On 7.6.1

Via RHSA-2022:7417 https://access.redhat.com/errata/RHSA-2022:7417

Note

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