Bug 2381861 (CVE-2025-7784) - CVE-2025-7784 org.keycloak/keycloak-services: Privilege Escalation in Keycloak Admin Console (FGAPv2 Enabled)

Keywords: Security

Status: NEW

Alias: CVE-2025-7784

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: 2025-07-18 06:06 UTC by OSIDB Bzimport

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

CC List: 26 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2025:12015	0	None	None	None	2025-07-29 01:35:28 UTC
Red Hat Product Errata	RHSA-2025:12016	0	None	None	None	2025-07-29 01:45:58 UTC

OSIDB Bzimport 2025-07-18 06:06:49 UTC Description

A Privilege Escalation vulnerability was identified in the Keycloak identity and access management solution, specifically when FGAPv2 is enabled in version 26.2.x. The flaw lies in the admin permission enforcement logic, where a user with manage-users privileges can self-assign realm-admin rights. The escalation occurs due to missing privilege boundary checks in role mapping operations via the admin REST interface. A malicious administrator with limited permissions can exploit this by editing their own user roles, gaining unauthorized full access to realm configuration and user data.

errata-xmlrpc 2025-07-29 01:35:25 UTC Comment 2

This issue has been addressed in the following products:

  Red Hat build of Keycloak 26

Via RHSA-2025:12015 https://access.redhat.com/errata/RHSA-2025:12015

errata-xmlrpc 2025-07-29 01:45:56 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat build of Keycloak 26.2

Via RHSA-2025:12016 https://access.redhat.com/errata/RHSA-2025:12016

Note

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