Keycloak: phishing attack via email verification step in first login flow

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-7365
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-10 15:15:30 UTC
Updated	2026-05-06 17:16:19 UTC
Description	A flaw was found in Keycloak. When an authenticated attacker attempts to merge accounts with another existing account d

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

Problem Types: CWE-346 | CWE-346 Origin Validation Error

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
3.1	secalert@redhat.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Keycloak	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Keycloak 26	Not specified	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26	Not specified	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0.13-2 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0-16 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0-17 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2.6-1 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2-6 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2-6 * rpm	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2025:12016	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2025:11986	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2025:12015	secalert@redhat.com	access.redhat.com	Vendor Advisory
github.com/keycloak/keycloak/pull/40520	secalert@redhat.com	github.com	
access.redhat.com/errata/RHSA-2025:11987	secalert@redhat.com	access.redhat.com	Vendor Advisory
github.com/keycloak/keycloak/issues/40446	secalert@redhat.com	github.com	
access.redhat.com/security/cve/CVE-2025-7365	secalert@redhat.com	access.redhat.com	Vendor Advisory
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-07-08T18:35:00.135Z	Reported to Red Hat.
CNA	2025-06-20T00:00:00.000Z	Made public.

Workarounds

CNA: Disable account review in the Identity Provider to prevent users from potentially modifying identity information. Disable the email verification step and use only re-authentication step.

There are currently no legacy QID mappings associated with this CVE.