CVE-2025-7365

VEX

Public on June 20, 2025

Last modified: January 8, 2026 at 2:59:40 AM UTC

MODERATE

Moderate severity

What does this mean?

7.1

CVSS v3 Score Breakdown

Jump to section

Description | Statement | Mitigation | Additional information | Affected Packages | CVSS Score Details | Weakness (CWE) | FAQ

Description

A flaw was found in Keycloak. When an authenticated attacker attempts to merge accounts with another existing account during an identity provider (IdP) login, the attacker will subsequently be prompted to "review profile" information. This vulnerability allows the attacker to modify their email address to match that of a victim's account, triggering a verification email sent to the victim's email address. The attacker's email address is not present in the verification email content, making it a potential phishing opportunity. If the victim clicks the verification link, the attacker can gain access to the victim's account.

Statement

To exploit this vulnerability, IdP must be configured in Keycloak and the attacker would require both a registered Keycloak and identity provider account. Additionally, an attacker would need to know the email or Keycloak username of the victim. Finally, the victim would need to accept the verification link within the 5 minutes that the token is active.

Mitigation

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.

Additional information

- Bugzilla 2378852: keycloak: Phishing attack via email verification step in first login flow
- CWE-346: Origin Validation Error

External references

- https://www.cve.org/CVERecord?id=CVE-2025-7365
- https://nvd.nist.gov/vuln/detail/CVE-2025-7365

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State | Errata | Clear all

Products / Services	Red Hat build of Keycloak 26
Components	org.keycloak/keycloak-services

State	Fixed
Justification	None
Errata	RHSA-2025:11987
Release Date	July 28, 2025

Products / Services	Red Hat build of Keycloak 26
Components	org.keycloak/keycloak-services
State	Fixed
Justification	None
Errata	RHSA-2025:12015
Release Date	July 29, 2025

Products / Services	Red Hat build of Keycloak 26.0

1-10 of 8

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	7.1	7.1
Attack Vector	Network	Network
Attack Complexity	High	High
Privileges Required	Low	Low
User Interaction	Required	Required
Scope	Unchanged	Unchanged
Confidentiality Impact	High	High
Integrity Impact	High	High
Availability Impact	High	High

CVSS v3 Vector

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

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

Frequently Asked Questions

- Why is Red Hat's CVSS v3 score or Impact different from other vendors?
- My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?
- What can I do if my product is listed as "Will not fix"?
- What can I do if my product is listed as "Fix deferred"?
- What is a mitigation?
- I have a Red Hat product but it is not in the above list, is it affected?
- Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: January 8, 2026 at 2:59:40 AM UTC

Site Info

Related Sites

All systems operational