Bug 2378852 (CVE-2025-7365) - CVE-2025-7365 keycloak: Phishing attack via email verification step in first login flow

Keywords: Security

Status: NEW

Alias: CVE-2025-7365

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: 2025-07-08 20:32 UTC by OSIDB Bzimport

Modified: 2025-07-29 01:45 UTC (History)

CC List: 7 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-2025:11986	0	None	None	None	2025-07-28 16:46:52 UTC
Red Hat Product Errata	RHSA-2025:11987	0	None	None	None	2025-07-28 16:43:49 UTC
Red Hat Product Errata	RHSA-2025:12015	0	None	None	None	2025-07-29 01:35:26 UTC

Red Hat Product Errata	RHSA-2025:12016	0	None	None	None	2025-07-29 01:45:57 UTC

OSIDB Bzimport 2025-07-08 20:32:39 UTC Description

```
There is a flaw with the first login flow where, during a IdP
login, an attacker with a registered account can initiate the
process to merge accounts with an existing victim's account.
The attacker will subsequently be prompted to "review profile"
information, which allows the the attacker to modify their
email address to that of a victim's account. This triggers a
verification email sent to the victim's email address. If the
victim clicks the verification link, the attacker can gain
access to the victim's account. While not a zero-interaction
attack, the attacker's email address is not directly present
in the verification email content, making it a potential
phishing opportunity.
```

errata-xmlrpc 2025-07-28 16:43:48 UTC Comment 1

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

  Red Hat build of Keycloak 26

Via RHSA-2025:11987 https://access.redhat.com/errata/RHSA-
2025:11987
```

errata-xmlrpc 2025-07-28 16:46:51 UTC Comment 2

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

  Red Hat build of Keycloak 26.0

Via RHSA-2025:11986 https://access.redhat.com/errata/RHSA-
2025:11986
```

errata-xmlrpc 2025-07-29 01:35:25 UTC Comment 3

```
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 4

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.