



# Bug 2253952 (CVE-2023-6717) - CVE-2023-6717 keycloak: XSS via assertion consumer service URL in SAML POST-binding flow

**Keywords:** Security

**Reported:** 2023-12-11 08:34 UTC by TEJ RATHI

**Status:** NEW

**Modified:** 2026-04-30 04:01 UTC [\(History\)](#)

**Alias:** CVE-2023-6717

**CC List:** 91 users [\(show\)](#)

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Version:** unspecified

**Environment:**

**Hardware:** All

**Last Closed:**

**OS:** Linux

**Embargoed:**

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:**

**Blocks:** 2253608

**TreeView+** [depends on](#) / [blocked](#)

| Attachments | <a href="#">(Terms of Use)</a> |
|-------------|--------------------------------|
|             |                                |

## Links

| System                 | ID                             | Private | Priority | Status | Summary | Last Updated            |
|------------------------|--------------------------------|---------|----------|--------|---------|-------------------------|
| Red Hat Product Errata | <a href="#">RHSA-2024:1867</a> | 0       | None     | None   | None    | 2024-04-16 20:27:01 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2024:1868</a> | 0       | None     | None   | None    | 2024-04-16 20:26:33 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2024:2945</a> | 0       | None     | None   | None    | 2024-05-21 14:18:48 UTC |

|                        |                                |   |      |      |      |                         |
|------------------------|--------------------------------|---|------|------|------|-------------------------|
| Red Hat Product Errata | <a href="#">RHSA-2024:4057</a> | 0 | None | None | None | 2024-06-24 01:38:34 UTC |
|------------------------|--------------------------------|---|------|------|------|-------------------------|

TEJ RATHI 2023-12-11 08:34:32 UTC

[Description](#)

Keycloak allows arbitrary URLs as SAML Assertion Consumer Service POST Binding URL (ACS), including JavaScript URIs (javascript:). Allowing JavaScript URIs in combination with HTML forms leads to JavaScript evaluation in the context of the embedding origin on form submission. Thus, Keycloak is vulnerable to Cross-Site Scripting (XSS) by registering a JavaScript URI as Assertion Consumer Service POST Binding URL.

errata-xmlrpc 2024-04-16 20:26:29 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 22.0.10

Via [RHSA-2024:1868](#) <https://access.redhat.com/errata/RHSA-2024:1868>

errata-xmlrpc 2024-04-16 20:26:58 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 22

Via [RHSA-2024:1867](#) <https://access.redhat.com/errata/RHSA-2024:1867>

errata-xmlrpc 2024-05-21 14:18:42 UTC

[Comment 12](#)

This issue has been addressed in the following products:

Red Hat JBoss AMQ

Via [RHSA-2024:2945](#) <https://access.redhat.com/errata/RHSA-2024:2945>

errata-xmlrpc 2024-06-24 01:38:30 UTC

[Comment 15](#)

This issue has been addressed in the following products:

RHOSS-1.33-RHEL-8

Via RHSA-2024:4057 <https://access.redhat.com/errata/RHSA-2024:4057>

---

Note

You need to [log in](#) before you can comment on or make changes to this bug.

