



# Bug 2311641 (CVE-2024-8698) - CVE-2024-8698 keycloak-saml-core: Improper Verification of SAML Responses Leading to Privilege Escalation in Keycloak

**Keywords:** Security

**Reported:** 2024-09-11 13:13 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-04-01 08:28 UTC ([History](#))

**Alias:** CVE-2024-8698

**CC List:** 39 users ([show](#))

**Deadline:** 2024-09-19

**Fixed In Version:**

**Product:** Security Response

**Clone Of:**

**Component:** vulnerability

**Environment:**

**Last Closed:**

**Embargoed:**

**Version:** unspecified

**Hardware:** All

**OS:** Linux

**Priority:** high

**Severity:** high

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:**

**Blocks:**


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

## Attachments [\(Terms of Use\)](#)

### Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	<a href="#">RHSA-2024:6878</a>	0	None	None	None	2024-09-19 16:41:18 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:6879</a>	0	None	None	None	2024-09-19 16:41:23 UTC
Red Hat	<a href="#">RHSA-2024:6880</a>	0	None	None	None	2024-09-19

Product Errata						16:41:36 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:6882</a>	0	None	None	None	2024-09-19 16:45:48 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:6886</a>	0	None	None	None	2024-09-19 16:54:31 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:6887</a>	0	None	None	None	2024-09-19 17:07:02 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:6888</a>	0	None	None	None	2024-09-19 17:02:45 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:6889</a>	0	None	None	None	2024-09-19 17:10:47 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:6890</a>	0	None	None	None	2024-09-19 17:06:36 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:8823</a>	0	None	None	None	2024-11-04 20:12:13 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:8824</a>	0	None	None	None	2024-11-04 20:11:43 UTC
Red Hat Product Errata	<a href="#">RHSA-2024:8826</a>	0	None	None	None	2024-11-04 20:56:42 UTC

OSIDB Bzimport  2024-09-11 13:13:17 UTC[Description](#)

The SAML signature validation method in Keycloak uses the position of the signature within the XML document to determine if the signature is for the full document or an assertion. This approach can be exploited by attackers to bypass signature validation and perform unauthorized actions.

errata-xmlrpc 2024-09-19 16:41:16 UTC

[Comment 2](#)

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 7

Via RHSA-2024:6878 <https://access.redhat.com/errata/RHSA-2024:6878>

errata-xmlrpc 2024-09-19 16:41:21 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 8

Via RHSA-2024:6879 <https://access.redhat.com/errata/RHSA-2024:6879>

errata-xmlrpc 2024-09-19 16:41:34 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 9

Via RHSA-2024:6880 <https://access.redhat.com/errata/RHSA-2024:6880>

errata-xmlrpc 2024-09-19 16:45:46 UTC

[Comment 5](#)

This issue has been addressed in the following products:

RHEL-8 based Middleware Containers

Via RHSA-2024:6882 <https://access.redhat.com/errata/RHSA-2024:6882>

errata-xmlrpc 2024-09-19 16:54:28 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat Single Sign-On

Via RHSA-2024:6886 <https://access.redhat.com/errata/RHSA-2024:6886>

errata-xmlrpc 2024-09-19 17:02:43 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 22

Via RHSA-2024:6888 <https://access.redhat.com/errata/RHSA-2024:6888>

errata-xmlrpc 2024-09-19 17:06:34 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 22

Via RHSA-2024:6890 <https://access.redhat.com/errata/RHSA-2024:6890>

errata-xmlrpc 2024-09-19 17:06:59 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 22

Via RHSA-2024:6887 <https://access.redhat.com/errata/RHSA-2024:6887>

errata-xmlrpc 2024-09-19 17:10:44 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 24

Via RHSA-2024:6889 <https://access.redhat.com/errata/RHSA-2024:6889>

errata-xmlrpc 2024-11-04 20:11:41 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 9

Via RHSA-2024:8824 <https://access.redhat.com/errata/RHSA-2024:8824>

errata-xmlrpc 2024-11-04 20:12:10 UTC

[Comment 12](#)

This issue has been addressed in the following products:

Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 8

Via RHSA-2024:8823 <https://access.redhat.com/errata/RHSA-2024:8823>

errata-xmlrpc 2024-11-04 20:56:40 UTC

[Comment 13](#)

This issue has been addressed in the following products:

Red Hat JBoss Enterprise Application Platform

Via RHSA-2024:8826 <https://access.redhat.com/errata/RHSA-2024:8826>

---

**Note**

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

