



Bug 2302064 (CVE-2024-7341) - CVE-2024-7341 wildfly-elytron: org.keycloak/keycloak-services: session fixation in elytron saml adapters

Keywords: Security ✕

Reported: 2024-07-31 15:15 UTC by Robb Gatica

Status: NEW

Modified: 2026-04-01 08:29 UTC [\(History\)](#)

Alias: CVE-2024-7341

CC List: 42 users ([show](#))

Deadline: 2024-09-09

Product: Security Response

Fixed In Version:

Clone Of:

Component: vulnerability

Environment:

Last Closed:

Embargoed:

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](#)

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

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2024:6493	0	None	None	None	2024-09-09 15:58:44 UTC
Red Hat Product Errata	RHSA-2024:6494	0	None	None	None	2024-09-09 16:00:17 UTC
Red Hat	RHSA-2024:6495	0	None	None	None	2024-09-09

Product Errata						16:07:52 UTC
Red Hat Product Errata	RHSA-2024:6497	0	None	None	None	2024-09-09 16:12:29 UTC
Red Hat Product Errata	RHSA-2024:6499	0	None	None	None	2024-09-09 15:58:22 UTC
Red Hat Product Errata	RHSA-2024:6500	0	None	None	None	2024-09-09 16:06:02 UTC
Red Hat Product Errata	RHSA-2024:6501	0	None	None	None	2024-09-09 16:02:04 UTC
Red Hat Product Errata	RHSA-2024:6502	0	None	None	None	2024-09-09 16:05:32 UTC
Red Hat Product Errata	RHSA-2024:6503	0	None	None	None	2024-09-09 16:05:55 UTC

Robb Gatica 2024-07-31 15:15:26 UTC

[Description](#)

The SAML adapter is expected to change the session ID (and the respective JSESSIONID cookie) when the login is performed (except if the option `turnOffChangeSessionIdOnLogin` is true). This way the session ID is modified in the login to change the previous non-authenticated ID to a new one and avoid using the same value (just to protect against a possible cookie hijacking).

Requirements to exploit:

You need to hijack the current session before authentication and it will be valid after it. Session fixation issue.

Component affected:
org.keycloak.services

Version affected: <= 25.0.2 (also present in RHBK and RHSSO elytron variant).

errata-xmlrpc 2024-09-09 15:58:19 UTC

[Comment 1](#)

This issue has been addressed in the following products:

Red Hat Single Sign-On

Via RHSA-2024:6499 <https://access.redhat.com/errata/RHSA-2024:6499>

errata-xmlrpc 2024-09-09 15:58:42 UTC

[Comment 2](#)

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 7

Via RHSA-2024:6493 <https://access.redhat.com/errata/RHSA-2024:6493>

errata-xmlrpc 2024-09-09 16:00:14 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 8

Via RHSA-2024:6494 <https://access.redhat.com/errata/RHSA-2024:6494>

errata-xmlrpc 2024-09-09 16:02:02 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 22

Via RHSA-2024:6501 <https://access.redhat.com/errata/RHSA-2024:6501>

errata-xmlrpc 2024-09-09 16:05:29 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 24

Via RHSA-2024:6502 <https://access.redhat.com/errata/RHSA-2024:6502>

errata-xmlrpc 2024-09-09 16:05:52 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 22

Via RHSA-2024:6503 <https://access.redhat.com/errata/RHSA-2024:6503>

errata-xmlrpc 2024-09-09 16:06:00 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat build of Keycloak 22

Via RHSA-2024:6500 <https://access.redhat.com/errata/RHSA-2024:6500>

errata-xmlrpc 2024-09-09 16:07:50 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.6 for RHEL 9

Via RHSA-2024:6495 <https://access.redhat.com/errata/RHSA-2024:6495>

errata-xmlrpc 2024-09-09 16:12:26 UTC

[Comment 9](#)

This issue has been addressed in the following products:

RHEL-8 based Middleware Containers

Via RHSA-2024:6497 <https://access.redhat.com/errata/RHSA-2024:6497>

Patricia Sheats 2024-10-16 10:07:43 UTC

[Comment 10](#)

(In reply to errata-xmlrpc from [comment #9](#))
> This issue has been addressed in the following products:
>
> RHEL-8 based Middleware Containers
>
> Via RHSA-2024:6497 <https://access.redhat.com/errata/RHSA-2024:6497> <https://101games.io>

Yes

Note

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

