Bug 2331178 (CVE-2024-12369) - CVE-2024-12369 elytron-oidc-client: OIDC Authorization Code Injection

Keywords: Security

Status: NEW

Alias: CVE-2024-12369

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: 2024-12-09 16:38 UTC by OSIDB Bzimport

Modified: 2026-04-30 04:00 UTC (History)

CC List: 30 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-2025:3989	0	None	None	None	2025-04-17 14:31:25 UTC
Red Hat Product Errata	RHSA-2025:3990	0	None	None	None	2025-04-17 14:31:51 UTC
Red Hat Product Errata	RHSA-2025:3992	0	None	None	None	2025-04-17 14:38:09 UTC

OSIDB Bzimport 2024-12-09 16:38:34 UTC Description

When using the RH SSO OIDC adapter with EAP 7.x or when using the elytron-oidc-client subsystem with EAP 8.x, there is a potential for authorization code injection attacks. That means that an attacker can inject a stolen authorization code into the attacker's own session with the client. This allows the attacker to associate its session with the client with a victim's identity.

Requirements to exploit:

* The attacker needs to obtain an authorization code from an authorization response sent to the client.
* The attacker can then access the application and start the login process with the legitimate client.
* In the response of the OpenID provider to the legitimate client, the attacker can replace the newly sent authorization code with the previously stolen authorization code.
* The legitimate client will send that stolen authorization code and along with its credentials to the OpenID provider to exchange the code for a token.
* The OpenID provider's checks will succeed and a token will be issued to the client.
* The attacker has now associated their session with the victim's identity.

errata-xmlrpc 2025-04-17 14:31:23 UTC Comment 8

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 8

Via RHSA-2025:3989 https://access.redhat.com/errata/RHSA-2025:3989

errata-xmlrpc 2025-04-17 14:31:48 UTC Comment 9

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 8.0 for RHEL 9

Via RHSA-2025:3990 https://access.redhat.com/errata/RHSA-2025:3990

errata-xmlrpc 2025-04-17 14:38:07 UTC Comment 10

This issue has been addressed in the following products:

Red Hat JBoss Enterprise Application Platform

Via RHSA-2025:3992 https://access.redhat.com/errata/RHSA-2025:3992

Note

You need to log in before you can comment on or make changes to this bug.