Bug 2262918 (CVE-2024-1249) - CVE-2024-1249 keycloak: org.keycloak.protocol.oidc: unvalidated cross-origin messages in checkLoginIframe leads to DDoS

Keywords: Security ×

Status: NEW

Alias: CVE-2024-1249

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks: 2262938

TreeView+ depends on / blocked

Reported: 2024-02-06 05:54 UTC by TEJ RATHI

Modified: 2026-04-01 08:29 UTC (History)

CC List: 74 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-2024:1860	0	None	None	None	2024-04-16 19:52:27 UTC
Red Hat Product Errata	RHSA-2024:1861	0	None	None	None	2024-04-16 19:52:43 UTC
Red Hat Product Errata	RHSA-2024:1862	0	None	None	None	2024-04-16 19:52:57 UTC

Red Hat Product Errata	RHSA-2024:1864	0	None	None	None	2024-04-16 19:54:28 UTC
Red Hat Product Errata	RHSA-2024:1866	0	None	None	None	2024-04-16 20:04:41 UTC
Red Hat Product Errata	RHSA-2024:1867	0	None	None	None	2024-04-16 20:26:54 UTC
Red Hat Product Errata	RHSA-2024:1868	0	None	None	None	2024-04-16 20:26:38 UTC
Red Hat Product Errata	RHSA-2024:2945	0	None	None	None	2024-05-21 14:18:58 UTC
Red Hat Product Errata	RHSA-2024:4057	0	None	None	None	2024-06-24 01:38:35 UTC
Red Hat Product Errata	RHSA-2025:9582	0	None	None	None	2025-06-25 00:20:31 UTC
Red Hat Product Errata	RHSA-2025:9583	0	None	None	None	2025-06-25 00:15:14 UTC

TEJ RATHI 2024-02-06 05:54:00 UTC Description

```
A potential security flaw in the "checkLoginIframe" which
allows unvalidated cross-origin messages, enabling potential
DDoS attacks. By exploiting this vulnerability, attackers
could coordinate to send millions of requests in seconds using
simple code, significantly impacting the application's
availability without proper origin validation for incoming
messages.

Component affected: org.keycloak.protocol.oidc
Version affected: <= 23.0.6
```

TEJ RATHI 2024-02-06 12:20:23 UTC Comment 6

```
Update: Version affected: <= 23.0.6

Initially we received wrong versions in the original report.
```

Updated in Comment 0 as well.

errata-xmlrpc 2024-04-16 19:52:24 UTC Comment 8

This issue has been addressed in the following products:

  Red Hat Single Sign-On 7.6 for RHEL 7

Via RHSA-2024:1860 https://access.redhat.com/errata/RHSA-2024:1860

errata-xmlrpc 2024-04-16 19:52:39 UTC Comment 9

This issue has been addressed in the following products:

  Red Hat Single Sign-On 7.6 for RHEL 8

Via RHSA-2024:1861 https://access.redhat.com/errata/RHSA-2024:1861

errata-xmlrpc 2024-04-16 19:52:53 UTC Comment 10

This issue has been addressed in the following products:

  Red Hat Single Sign-On 7.6 for RHEL 9

Via RHSA-2024:1862 https://access.redhat.com/errata/RHSA-2024:1862

errata-xmlrpc 2024-04-16 19:54:25 UTC Comment 11

This issue has been addressed in the following products:

  RHEL-8 based Middleware Containers

Via RHSA-2024:1864 https://access.redhat.com/errata/RHSA-2024:1864

errata-xmlrpc 2024-04-16 20:04:38 UTC Comment 12

This issue has been addressed in the following products:

RHSSO 7.6.8

Via RHSA-2024:1866 https://access.redhat.com/errata/RHSA-2024:1866

errata-xmlrpc 2024-04-16 20:26:35 UTC Comment 13

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 20:26:51 UTC Comment 14

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 14:18:54 UTC Comment 15

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 01:38:31 UTC Comment 16

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

errata-xmlrpc 2025-06-25 00:15:09 UTC Comment 19

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 7.3 EUS for RHEL 7

Via RHSA-2025:9583 https://access.redhat.com/errata/RHSA-2025:9583

errata-xmlrpc 2025-06-25 00:20:26 UTC Comment 20

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 7.1 EUS for RHEL 7

Via RHSA-2025:9582 https://access.redhat.com/errata/RHSA-2025:9582

Note

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