



Bug 2302487 (CVE-2024-7409) - CVE-2024-7409 QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server During Socket Closure

Keywords: Security

Reported: 2024-08-02 11:35 UTC by Michal Findra

Status: NEW

Modified: 2024-12-12 02:08 UTC [\(History\)](#)

Alias: CVE-2024-7409

CC List: 12 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 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-2024:10518	0	None	None	None	2024-12-03 18:08:17 UTC
Red Hat Product Errata	RHSA-2024:10528	0	None	None	None	2024-12-04 04:02:02 UTC
Red Hat Product Errata	RHSA-2024:10813	0	None	None	None	2024-12-12 02:08:20 UTC

Red Hat Product Errata	RHSA-2024:6811	0	None	None	None	2024-09-25 01:07:00 UTC
Red Hat Product Errata	RHSA-2024:6818	0	None	None	None	2024-09-25 13:59:35 UTC
Red Hat Product Errata	RHSA-2024:6824	0	None	None	None	2024-09-24 15:28:14 UTC
Red Hat Product Errata	RHSA-2024:6964	0	None	None	None	2024-09-24 03:22:43 UTC
Red Hat Product Errata	RHSA-2024:7408	0	None	None	None	2024-10-01 02:43:47 UTC
Red Hat Product Errata	RHSA-2024:8991	0	None	None	None	2024-11-13 18:35:22 UTC
Red Hat Product Errata	RHSA-2024:9136	0	None	None	None	2024-11-12 08:56:06 UTC
Red Hat Product Errata	RHSA-2024:9620	0	None	None	None	2024-11-20 04:18:22 UTC
Red Hat Product Errata	RHSA-2024:9912	0	None	None	None	2024-11-19 02:29:50 UTC

Michal Findra 2024-08-02 11:35:01 UTC

[Description](#)

A flaw was discovered in the qemu code for temporarily exposing an NBD server (used for storage migration and other tasks), where qemu can crash if a client still has a socket open at the time the server is taken offline. Even when qemu is set up to only accept clients with proper TLS credentials, an attacker without the TLS credentials can exploit the flaw by connecting a second socket while a storage migration is ongoing through the intended socket, where the attacker then stalls the NBD handshake to not reach the point of the TLS negotiation, then waiting for the server to go offline. When the NBD

server is stopped, closing the attacker's socket can cause qemu to crash, forming a denial of service attack.

errata-xmlrpc 2024-09-24 03:22:42 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2024:6964 <https://access.redhat.com/errata/RHSA-2024:6964>

errata-xmlrpc 2024-09-24 15:28:12 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.16

Via RHSA-2024:6824 <https://access.redhat.com/errata/RHSA-2024:6824>

errata-xmlrpc 2024-09-25 01:06:58 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.13

Via RHSA-2024:6811 <https://access.redhat.com/errata/RHSA-2024:6811>

errata-xmlrpc 2024-09-25 13:59:33 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.15

Via RHSA-2024:6818 <https://access.redhat.com/errata/RHSA-2024:6818>

errata-xmlrpc 2024-10-01 02:43:45 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.2 Extended Update Support

Via RHSA-2024:7408 <https://access.redhat.com/errata/RHSA-2024:7408>

errata-xmlrpc 2024-11-12 08:56:04 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2024:9136 <https://access.redhat.com/errata/RHSA-2024:9136>

errata-xmlrpc 2024-11-13 18:35:20 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.15

Via RHSA-2024:8991 <https://access.redhat.com/errata/RHSA-2024:8991>

errata-xmlrpc 2024-11-19 02:29:48 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2024:9912 <https://access.redhat.com/errata/RHSA-2024:9912>

errata-xmlrpc 2024-11-20 04:18:21 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.14

Via RHSA-2024:9620 <https://access.redhat.com/errata/RHSA-2024:9620>

errata-xmlrpc 2024-12-03 18:08:15 UTC

[Comment 12](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.17

Via RHSA-2024:10518 <https://access.redhat.com/errata/RHSA-2024:10518>

errata-xmlrpc 2024-12-04 04:02:00 UTC

[Comment 13](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.16

Via RHSA-2024:10528 <https://access.redhat.com/errata/RHSA-2024:10528>

errata-xmlrpc 2024-12-12 02:08:19 UTC

[Comment 14](#)

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.13

Via RHSA-2024:10813 <https://access.redhat.com/errata/RHSA-2024:10813>

Note

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

