Bug 2408845 (CVE-2025-12464) - CVE-2025-12464 qemu-kvm: Stack buffer overflow in e1000 device via short frames in loopback mode

Keywords: Security ×

Status: NEW

Alias: CVE-2025-12464

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: 2408852 2408853 ~~2408851~~

Blocks:

TreeView+ depends on / blocked

Reported: 2025-10-31 13:09 UTC by OSIDB Bzimport

Modified: 2025-11-05 16:55 UTC (History)

CC List: 11 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2025-10-31 13:09:34 UTC Description

A stack-based buffer overflow was found in the QEMU e1000 network device. The code for padding short frames was dropped from individual network devices and moved to the net core code. The issue stems from the device's receive code still being able to process a short frame in loopback mode. This could lead to a buffer overrun in the e1000_receive_iov() function via the loopback code path. A malicious guest user could use this vulnerability to crash the QEMU process on the host, resulting in a denial of service.

Upstream issue:
https://gitlab.com/qemu-project/qemu/-/issues/3043

Patch:
https://lore.kernel.org/qemu-devel/20251028160042.3321933-1-peter.maydell@linaro.org/T/#u

Note

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