CVE-2014-0077

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-0077
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-14 23:55:07 UTC
Updated	2026-05-06 22:30:45 UTC
Description	drivers/vhost/net.c in the Linux kernel before 3.13.10, when mergeable buffers are disabled, does not properly validate pack

Risk And Classification

Primary CVSS: v2.0 5.5 from nvd@nist.gov

AV:A/AC:H/Au:S/C:P/I:P/A:C

Problem Types: CWE-787 | n/a

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

High

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Complete

AV:A/AC:H/Au:S/C:P/I:P/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Bug 1064440 – CVE-2014-0077 kernel: vhost-net: insufficiency in handling of big packets in handle_rx()	af854a3a-2127-422b-91ae-364da2
vhost: fix total length when packets are too short · torvalds/linux@d8316f3 · GitHub	af854a3a-2127-422b-91ae-364da2
Linux Kernel 'handle_rx()' Function Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-91ae-364da2
Security Advisory SA59599 - Ubuntu update for kernel - Secunia	af854a3a-2127-422b-91ae-364da2
www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.13.10	af854a3a-2127-422b-91ae-364da2
About Secunia Research | Flexera	af854a3a-2127-422b-91ae-364da2
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.