CVE-2014-0038

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

Summary

CVE	CVE-2014-0038
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-06 22:55:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The compat_sys_recvmmsg function in net/compat.c in the Linux kernel before 3.13.2, when CONFIG_X86_X32 is enablec

Risk And Classification

Primary CVSS: v2.0 6.9 from nvd@nist.gov

AV:L/AC:M/Au:N/C:C/I:C/A:C

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:M/Au:N/C:C/I:C/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
[security-announce] openSUSE-SU-2014:0205-1: important: kernel to 3.11.1
Linux Kernel 'compat_sys_recvmmsg()' Function Local Memory Corruption Vulnerability
kernel/git/torvalds/linux.git - Linux kernel source tree
saelo/cve-2014-0038 · GitHub
USN-2096-1: Linux kernel vulnerability | Ubuntu
Support / Security / Advisories / / MDVSA-2014:038 | Mandriva
USN-2094-1: Linux kernel (Raring HWE) vulnerability | Ubuntu
Linux Kernel 3.13.1 - 'Recvmmsg' Local Privilege Escalation (Metasploit) - Linux local Exploit
x86, x32: Correct invalid use of user timespec in the kernel · torvalds/linux@2def2ef · GitHub
Security Advisory SA56669 - Ubuntu update for kernel - Secunia
Linux Kernel 3.4 < 3.13.2 - Arbitrary write with CONFIG_X86_X32
pastebin.com/raw.php
Bug 1060023 – CVE-2014-0038 Kernel: 3.4+ arbitrary write with CONFIG_X86_X32
USN-2095-1: Linux kernel (Saucy HWE) vulnerability | Ubuntu
oss-security - Linux 3.4+: arbitrary write with CONFIG_X86_X32 (CVE-2014-0038)
Linux Kernel 3.4 < 3.13.2 - Local Root (CONFIG_X86_X32=y)
Issue 338594 - chromium - exploitable linux kernel (3.4+) write bug in net/compat.c:compat_sys_recvmmsg under CONFIG_X86_X32_ABI - A
[security-announce] openSUSE-SU-2014:0204-1: important: kernel: security
www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.13.2
kernel/git/torvalds/linux.git - Linux kernel source tree
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report