

CVE-2014-3153

Linux Kernel Privilege Escalation Vulnerability

CISA KEV since May 25, 2022

Actively exploited

Public exploit module (Metasploit)

The futex_requeue function in kernel/futex.c in the Linux kernel through 3.14.5 does not ensure that calls have two different futex addresses, which allows local users to gain privileges via a crafted FUTEX_REQUEUE command that facilitates unsafe waiter modification.

EVRS

75/100

Urgent priority

CVSS V3.1

7.8

High · NVD

EPSS

0.372

98.5th percentile · FIRST

CISA DEADLINE

Jun 15, 2022

KEV since 2022 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.372 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 1 more affected product on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
linux kernel	< 3.2.60 ≥ 3.3 < 3.4.92 ≥ 3.5 < 3.10.42 ≥ 3.11 < 3.12.22 ≥ 3.13 < 3.14.6	no fixed version listed	NVD
enterprise linux server aus	6.2	no fixed version listed	NVD
opensuse	11.4	no fixed version listed	NVD
linux enterprise desktop	11	no fixed version listed	NVD
linux enterprise high availability extension	11	no fixed version listed	NVD
linux enterprise real time extension	11	no fixed version listed	NVD
linux enterprise server	11	no fixed version listed	NVD
ubuntu linux	12.04 14.04	no fixed version listed	NVD

Sources

Vendor guidance	git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit?id=13fbca4c6ecd96ec1a1cfa2e4f2ce191fe928a5e	NVD	nvd.nist.gov/vuln/detail/CVE-2014-3153
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2014-3171
Current data	evulnable.com/vulnerability-management/cve/CVE-2014-3153		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.