

CVE-2013-6282

Linux Kernel Improper Input Validation Vulnerability

CISA KEV since Sep 15, 2022

Actively exploited

Public exploit module (Metasploit)

The (1) get_user and (2) put_user API functions in the Linux kernel before 3.5.5 on the v6k and v7 ARM platforms do not validate certain addresses, which allows attackers to read or modify the contents of arbitrary kernel memory locations via a crafted application, as exploited in the wild against Android devices in October and November 2013.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.397 98.6th percentile · FIRST	CISA DEADLINE Oct 6, 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	0.397 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
linux kernel	< 3.2.54 ≥ 3.3 < 3.4.12 ≥ 3.5 < 3.5.5	no fixed version listed	NVD

Sources

Vendor guidance github.com/torvalds/linux/commit/8404663f81d212918ff85f493649a7991209fa04**git.kernel.org** git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=8404663f81d212918ff85f493649a7991209fa04
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2013-6282**NVD** nvd.nist.gov/vuln/detail/CVE-2013-6282**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2013-6110

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