

CVE-2013-2596

Linux Kernel Integer Overflow Vulnerability

CISA KEV since Sep 15, 2022

Actively exploited

Integer overflow in the fb_mmap function in drivers/video/fbmem.c in the Linux kernel before 3.8.9, as used in a certain Motorola build of Android 4.1.2 and other products, allows local users to create a read-write memory mapping for the entirety of kernel memory, and consequently gain privileges, via crafted /dev/graphics/fb0 mmap2 system calls, as demonstrated by the Motochopper pwn program.

EVRS 75_{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.032 88.1st 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	0.032 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
linux kernel	$\geq 2.6.12 < 3.0.75$ $\geq 3.1 < 3.2.45$ $\geq 3.3 < 3.4.42$ $\geq 3.5 < 3.8.9$	no fixed version listed	NVD
android	4.1.2	no fixed version listed	NVD
atrix hd	—	no fixed version listed	NVD
razr hd	—	no fixed version listed	NVD
razr m	—	no fixed version listed	NVD
msm8960	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/torvalds/linux/commit/b4cbb197c7e7a68dbad0d491242e3ca67420c13e

git.kernel.org git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=fc9bbca8f650e5f738af8806317c0a041a48ae4a

NVD nvd.nist.gov/vuln/detail/CVE-2013-2596

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2013-2538

Current data evulnable.com/vulnerability-management/cve/CVE-2013-2596

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