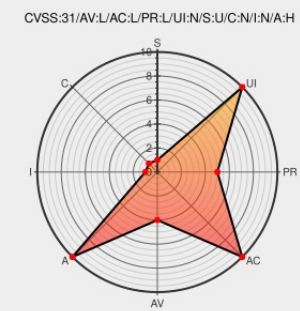
CVE-2023-3355

Published on: Not Yet Published

Last Modified on: 08/02/2023 03:42:00 PM UTC

CVE-2023-3355

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

A NULL pointer dereference flaw was found in the Linux kernel's drivers/gpu/drm/msm/msm_gem_submit.c code in the submit_lookup_cmds function, which fails because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system.

CVE-2023-3355 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
2217820 – (CVE-2023-3355) CVE-2023-3355 kernel: NULL pointer dereference in submit_lookup_cmds() in drivers/gpu/drm/msm/msm_gem_submit.c	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=2217820
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	MISC git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=d839f0811a31322c087a859c2b181e2383daa7be
cve-details	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2023-3355

CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

907070 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27363-1)

907219 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27366-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	6.1	-	All	All
Operating System	Linux	Linux Kernel	6.1	rc1	All	All
Operating System	Linux	Linux Kernel	6.1	rc2	All	All
Operating System	Linux	Linux Kernel	6.1	rc3	All	All
Operating System	Linux	Linux Kernel	6.1	rc4	All	All
Operating System	Linux	Linux Kernel	6.1	rc5	All	All
Operating System	Linux	Linux Kernel	6.1	rc6	All	All
Operating System	Linux	Linux Kernel	6.1	rc7	All	All

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:6.1:-:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:6.1:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:6.1:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:6.1:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:6.1:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:6.1:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:6.1:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:6.1:rc7:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-3355 : A NULL pointer dereference flaw was found in the #Linux #kernel's drivers/gpu/drm/msm/msm_gem_submi… twitter.com/i/web/status/1…	2023-06-28 21:04:09

← Previous ID

Next ID→