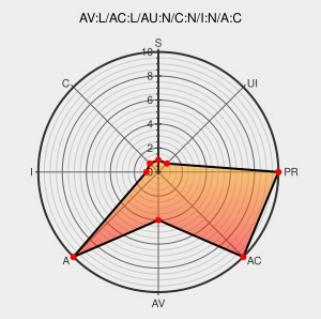
CVE-2013-4220

Published on: 08/24/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:45:00 AM UTC

CVE-2013-4220

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



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

The bad_mode function in arch/arm64/kernel/traps.c in the Linux kernel before 3.9.5 on the ARM64 platform allows local users to cause a denial of service (system crash) via vectors involving an attempted register access that triggers an unexpected value in the Exception Syndrome Register (ESR).

CVE-2013-4220 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
arm64: don't kill the kernel on a bad esr from el0 · torvalds/linux@9955ac4 · GitHub	Exploit, Patch, github.com, text/html	CONFIRM github.com/torvalds/linux/commit/9955ac47f4ba1c95ecb6092aeaefb40a22e99268
Bug 996380 – CVE-2013-4220 Kernel: arm64: unhandled esr by el0_sync_compat	bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=996380
kernel/git/torvalds/linux.git - Linux kernel source tree	web.archive.org, text/html, Inactive Link, Not Archived	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=9955ac47f4ba1c95ecb6092aeaefb40a22e99268
oss-security - Re: CVE	Patch	MLIST [oss-security] 20130808 Re: CVE Request: Linux kernel: arm64:

Request: Linux kernel: arm64: unhandled el0 traps	www.openwall.com text/html	unhandled el0 traps
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.9.5

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, 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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	3.9.0	All	All	All
Operating System	Linux	Linux Kernel	3.9.1	All	All	All
Operating System	Linux	Linux Kernel	3.9.2	All	All	All
Operating System	Linux	Linux Kernel	3.9.3	All	All	All
Operating System	Linux	Linux Kernel	3.9.0	All	All	All
Operating System	Linux	Linux Kernel	3.9.1	All	All	All
Operating System	Linux	Linux Kernel	3.9.2	All	All	All
Operating System	Linux	Linux Kernel	3.9.3	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:3.9.0:*:*:*:*:*:arm64:*:

cpe:2.3:o:linux:linux_kernel:3.9.1:*:*:*:*:*:arm64:*:

cpe:2.3:o:linux:linux_kernel:3.9.2:*:*:*:*:*:arm64:*:

cpe:2.3:o:linux:linux_kernel:3.9.3:*:*:*:*:*:arm64:*:

cpe:2.3:o:linux:linux_kernel:3.9.0:*:*:*:*:*:arm64:*:

cpe:2.3:o:linux:linux_kernel:3.9.1:*:*:*:*:*:arm64:*:

cpe:2.3:o:linux:linux_kernel:3.9.2:*:*:*:*:*:arm64:*:

cpe:2.3:o:linux:linux_kernel:3.9.3:*:*:*:*:*:arm64:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:arm64:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→