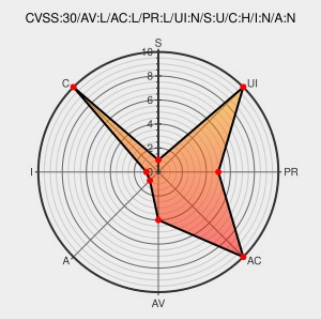
CVE-2014-9903

Published on: 06/27/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:59 PM UTC

CVE-2014-9903

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



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

The sched_read_attr function in kernel/sched/core.c in the Linux kernel 3.14-rc before 3.14-rc4 uses an incorrect size, which allows local users to obtain sensitive information from kernel stack memory via a crafted sched_getattr system call.

CVE-2014-9903 has been assigned by security@android.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	HIGH	NONE	NONE

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
Linux Kernel CVE-2014-9903 Local Information Disclosure Vulnerability	cve.report (archive) text/html	BID 91511
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory git.kernel.org	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=4efbc454ba68def5ef285b26ebfcfdb605b52755

	text/html	
sched: Fix information leak in sys_sched_getattr() · torvalds/linux@4efbc45 · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/4efbc454ba68def5ef285b26ebfcfdb605b52755

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	3.14	rc1	All	All
Operating System	Linux	Linux Kernel	3.14	rc2	All	All
Operating System	Linux	Linux Kernel	3.14	rc3	All	All
Operating System	Linux	Linux Kernel	3.14	rc1	All	All
Operating System	Linux	Linux Kernel	3.14	rc2	All	All
Operating System	Linux	Linux Kernel	3.14	rc3	All	All

cpe:2.3:o:linux:linux_kernel:3.14:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.14:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.14:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.14:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.14:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.14:rc3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report