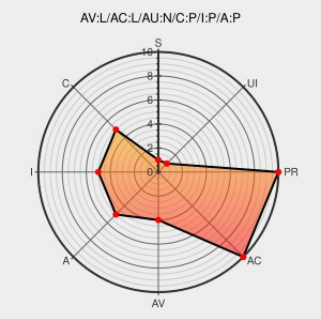
CVE-2014-4157

Published on: 06/23/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:43 PM UTC

CVE-2014-4157

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



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

arch/mips/include/asm/thread_info.h in the Linux kernel before 3.14.8 on the MIPS platform does not configure _TIF_SECCOMP checks on the fast system-call path, which allows local users to bypass intended PR_SET_SECCOMP restrictions by executing a crafted application without invoking a trace or audit subsystem.

CVE-2014-4157 has been assigned by security@debian.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
oss-security - Re: (Linux kernel) Bug#751417: linux-image-3.2.0-4-5kc-malta: no SIGKILL after prctl(PR_SET_SECCOMP, 1, ...) on MIPS	Mailing List, Third Party Advisory, www.openwall.com, text/html	MLIST [oss-security] 20140617 Re: (Linux kernel) Bug#751417: linux-image-3.2.0-4-5kc-malta: no SIGKILL after prctl(PR_SET_SECCOMP, 1, ...) on MIPS
	Vendor Advisory, www.kernel.org, text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.14.8
MIPS: asm: thread_info: Add _TIF_SECCOMP flag · torvalds/linux@137f7df · GitHub	Exploit, Patch, github.com, text/html	CONFIRM github.com/torvalds/linux/commit/137f7df8cead00688524c82360930845396b8a21

kernel/git/torvalds/linux.git - Linux kernel source tree	Exploit Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=137f7df8cead00688524c82360930845396b8a21
oss-security - Re: Bug#751417: linux-image-3.2.0-4-5kc-malta: no SIGKILL after prctl(PR_SET_SECCOMP, 1, ...) on MIPS	Mailing List Third Party Advisory openwall.com text/html	MLIST [oss-security] 20140616 Re: Bug#751417: linux-image-3.2.0-4-5kc-malta: no SIGKILL after prctl(PR_SET_SECCOMP, 1, ...) on MIPS
#751417 - linux-image-3.2.0-4-5kc-malta: no SIGKILL after prctl(PR_SET_SECCOMP, 1, ...) on MIPS (CVE-2014-4157) - Debian Bug report logs	Issue Tracking Mailing List Third Party Advisory bugs.debian.org text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=751417

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	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→