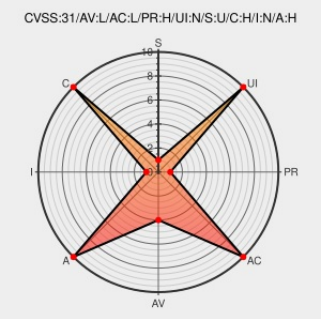
CVE-2011-2707

Published on: 05/24/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:20:00 AM UTC

CVE-2011-2707

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



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

The ptrace_setxregs function in arch/xtensa/kernel/ptrace.c in the Linux kernel before 3.1 does not validate user-space pointers, which allows local users to obtain sensitive information from kernel memory locations via a crafted PTRACE_SETXTREGS request.

CVE-2011-2707 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6 - MEDIUM

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

CVSS2 Score: 3.6 - LOW

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

CVE References

Description	Tags	Link
oss-security - Re: CVE request: kernel: arbitrary kernel read in xtensa	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20110720 Re: CVE request: kernel: arbitrary kernel read in xtensa

xtensa: prevent arbitrary read in ptrace · torvalds/linux@0d0138e · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/0d0138ebe24b94065580bd2601f8bb7eb6152f56
	Mailing List Patch Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.1
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=0d0138ebe24b94065580bd2601f8bb7eb6152f56

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→