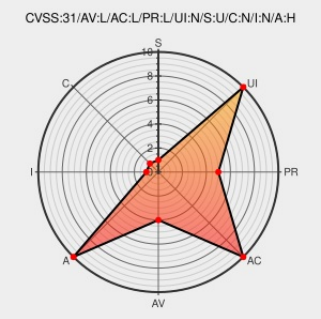
CVE-2011-2906

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

Last Modified on: 02/12/2023 08:15:00 PM UTC

CVE-2011-2906

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



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

** DISPUTED ** Integer signedness error in the pmcraid_ioctl_passthrough function in drivers/scsi/pmcraid.c in the Linux kernel before 3.1 might allow local users to cause a denial of service (memory consumption or memory corruption) via a negative size value in an ioctl call. NOTE: this may be a vulnerability only in unusual environments that provide a privileged program for obtaining the required file descriptor.

CVE-2011-2906 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

CVSS2 Score: 4.7 - MEDIUM

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

CVE References

Description	Tags	Link
oss-security - Re: CVE requests:	Mailing List	MLIST [oss-security] 20110810 Re: CVE requests: Two kernel issues

oss-security - Re: CVE requests: Two kernel issues	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20110810 Re: CVE requests: Two kernel issues
kernel/git/torvalds/linux.git - Linux kernel source tree	Mailing List Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=b5b515445f4f5a905c5dd27e6e682868ccd6c09d
	Mailing List Patch Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.1
[SCSI] pmcraid: reject negative request size · torvalds/linux@b5b5154 · GitHub	Exploit Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/b5b515445f4f5a905c5dd27e6e682868ccd6c09d

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→

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