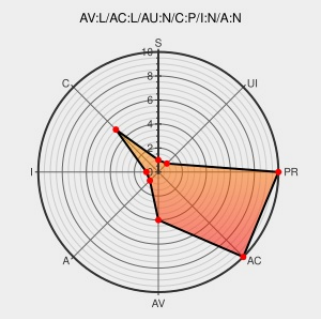
CVE-2011-2495

Published on: 06/13/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:18:00 AM UTC

CVE-2011-2495

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



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

fs/proc/base.c in the Linux kernel before 2.6.39.4 does not properly restrict access to /proc/#####/io files, which allows local users to obtain sensitive I/O statistics by polling a file, as demonstrated by discovering the length of another user's password.

CVE-2011-2495 has been assigned by secalert@redhat.com to track the vulnerability

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
oss-security - Re: CVE request: kernel: taskstats/procfs io infoleak	www.openwall.com text/html	MLIST [oss-security] 20110627 Re: CVE request: kernel: taskstats/procfs io infoleak
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch 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=1d1221f375c94ef961ba8574ac4f85c8870ddd51
access.redhat.com	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2011:1212
Bug 716825 – CVE-2011-2495 kernel: /proc/PID/io infoleak	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=716825

404 Not Found	ftp.osuosl.org text/plain Inactive Link Not Archived	CONFIRM ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39.4
proc: restrict access to /proc/PID/io · torvalds/linux@1d1221f · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/torvalds/linux/commit/1d1221f375c94ef961ba8574ac4f85c8870ddd51

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	2.6.39	All	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.39.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.39.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.39	All	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc4	All	All

Operating System	Linux	Linux Kernel	2.6.39	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.39.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.39.2	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:2.6.39:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39:rc7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.39.2:*:*:*:*:*:*:*:

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