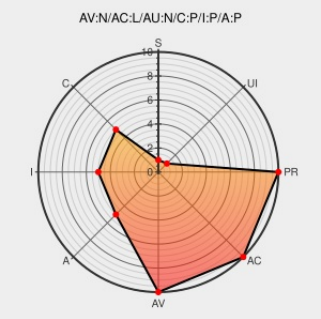
CVE-2004-2536

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2536

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



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

The exit_thread function (process.c) in Linux kernel 2.6 through 2.6.5 does not invalidate the per-TSS io_bitmap pointers if a process obtains IO access permissions from the ioperm function but does not drop those permissions when it exits, which allows other processes to access the per-TSS pointers, access restricted memory locations, and possibly gain privileges.

CVE-2004-2536 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Linux-Kernel Archive: Re: Bug in IO bitmap handling? Probably exploitable (2.6.5)	web.archive.org, text/html, Inactive Link, Not Archived	MLIST 20040507 Re: Bug in IO bitmap handling? Probably exploitable (2.6.5)
Linux Kernel Local IO Access Inheritance Vulnerability	cve.report (archive), text/html	BID 10302
Linux-Kernel Archive: Bug in IO bitmap handling? Probably exploitable (2.6.5)	Exploit, Patch, www.ussg.iu.edu, text/x-diff, Inactive Link, Not Archived	MLIST 20040507 Bug in IO bitmap handling? Probably exploitable (2.6.5)
Secunia - Advisories - Linux Kernel IO Bitmap Access	Vendor Advisory	SECUNIA 11577

Permissions Inheritance Vulnerability	web.archive.org text/html	
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF linux-exitthread-gain-privileges(16106)
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.6
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 5997

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	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All

Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All

cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.1:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→