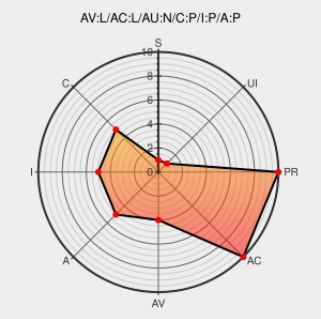
CVE-2008-3527

Published on: 11/05/2008 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:19:00 AM UTC

CVE-2008-3527

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



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

arch/i386/kernel/sysenter.c in the Virtual Dynamic Shared Objects (vDSO) implementation in the Linux kernel before 2.6.21 does not properly check boundaries, which allows local users to gain privileges or cause a denial of service via unspecified vectors, related to the install_special_mapping, syscall, and syscall32_nopage functions.

CVE-2008-3527 has been assigned by secalert@redhat.com 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
404: File not found	www.kernel.org text/plain Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.21
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:025	lists.opensuse.org text/html	SUSE SUSE-SR:2008:025
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 32759
kernel/git/torvalds/linux.git - Linux kernel source tree	web.archive.org text/html	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=7d91d531900bfa1165d445390b3b13a8013f98f7

	Inactive Link Not Archived	
Red hat update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 32485
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10602
Linux Kernel Virtual Dynamic Shared Objects Boundary Error May Let Local Users Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1021137
Bug 460251 – CVE-2008-3527 kernel: missing boundary checks in syscall/syscall32_nopage()	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=460251
About Secunia Research | Flexera	Vendor Advisory secunia.com Depreciated Link text/html	SECUNIA 33180
Support	www.redhat.com text/html	REDHAT RHSA-2008:0957
Debian -- Security Information -- DSA-1687-1 linux-2.6	www.debian.org Depreciated Link text/html	DEBIAN DSA-1687

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	2.2.27	All	All	All
Operating System	Linux	Linux Kernel	2.4.36	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.1	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.2	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.5	All	All	All

Operating System	Linux	Linux Kernel	2.4.36.6	All	All	All
Operating System	Linux	Linux Kernel	2.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.19.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.19	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.20	All	All	All
Operating System	Linux	Linux Kernel	2.2.27	All	All	All
Operating System	Linux	Linux Kernel	2.4.36	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.1	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.2	All	All	All

Operating System	Linux	Linux Kernel	2.4.36.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.5	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.6	All	All	All
Operating System	Linux	Linux Kernel	2.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.19.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.19	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.20	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:2.2.27:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.19.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.19.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.19.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.19.7:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.20.16:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.20.17:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.20.18:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.20.19:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.20.20:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.2.27:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.4.36.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:rc7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.19.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.19.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.19.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.19.7:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.20.16:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.20.17:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.20.18:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.20.19:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.20.20:*:*:*:*:*:*:*:

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

← Previous ID

Next ID→

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