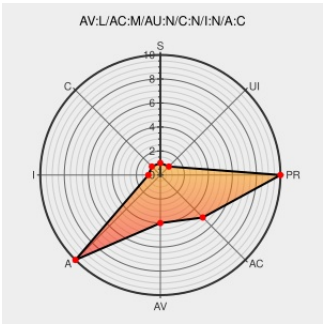
CVE-2009-4895

Published on: 09/08/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:23 PM UTC

CVE-2009-4895

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Race condition in the tty_fasync function in drivers/char/tty_io.c in the Linux kernel before 2.6.32.6 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via unknown vectors, related to the put_tty_queue and __f_setown functions. NOTE: the vulnerability was addressed in a different way in 2.6.32.9.

CVE-2009-4895 has been assigned by cve@mitre.org to track the vulnerability

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
559100 – (CVE-2009-4895) CVE-2009-4895 kernel: tty->pgrp races	Issue Tracking, Third Party Advisory, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=559100
USN-1000-1: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory, www.ubuntu.com, text/html	UBUNTU USN-1000-1
Bug 14605 – NULL Pointer Dereference drivers/char/n_tty.c	Issue Tracking, Patch, Vendor Advisory, bugzilla.kernel.org, text/html	CONFIRM bugzilla.kernel.org/show_bug.cgi?id=14605

	text/html	
oss-security - Re: CVE Request - kernel: put_tty_queue NULL pointer deref	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20100615 Re: CVE Request - kernel: put_tty_queue NULL pointer deref
oss-security - Re: CVE Request - kernel: put_tty_queue NULL pointer deref	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20100615 Re: CVE Request - kernel: put_tty_queue NULL pointer deref
oss-security - Re: CVE Request - kernel: put_tty_queue NULL pointer deref	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20100615 Re: CVE Request - kernel: put_tty_queue NULL pointer deref
Debian -- Security Information -- DSA-2094-1 linux-2.6	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-2094
404: File not found	Broken Link www.kernel.org text/plain Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.32.6
oss-security - CVE Request - kernel: put_tty_queue NULL pointer deref	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20100615 CVE Request - kernel: put_tty_queue NULL pointer deref
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=703625118069f9f8960d356676662d3db5a9d116

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating	Canonical	Ubuntu Linux	9.10	All	All	All

Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

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→