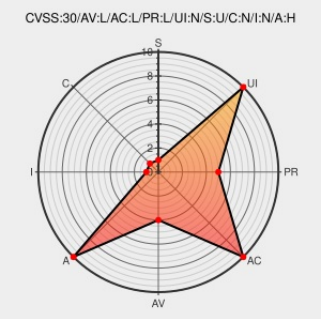
CVE-2011-5321

Published on: 05/02/2016 12:00:00 AM UTC

Last Modified on: 02/13/2023 03:06:56 AM UTC

CVE-2011-5321

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



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

The tty_open function in drivers/tty/tty_io.c in the Linux kernel before 3.1.1 mishandles a driver-lookup failure, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via crafted access to a device file under the /dev/pts directory.

CVE-2011-5321 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: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
oss-security - Re: CVE request: Linux kernel: tty: kobject reference leakage in tty_open	www.openwall.com text/html	MLIST [oss-security] 20150313 Re: CVE request: Linux kernel: tty: kobject reference leakage in tty_open

tty_open		
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c290f8358acaeffd8e0c551ddcc24d1206143376
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1221
Bug 1201887 – CVE-2011-5321 Kernel: tty: driver reference leakage in tty_open	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1201887
TTY: drop driver reference in tty_open fail path · torvalds/linux@c290f83 · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/c290f8358acaeffd8e0c551ddcc24d1206143376
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.1.1

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→