CVE-2009-1527

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-1527
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-05-05 20:30:00 UTC
Updated	2023-11-07 02:03:00 UTC
Description	Race condition in the ptrace_attach function in kernel/ptrace.c in the Linux kernel before 2.6.30-rc4 allows local users to gai

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.30	-	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.30	-	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc3	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source
wiki.rpath.com/Advisories:rPSA-2009-0084	CONFIRM
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM
oss-security - CVE request: kernel: ptrace_attach: fix the usage of ->cred_exec_mutex	MLIST
IBM X-Force Exchange	XF
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN

54188	OSVDB
SecurityFocus	BUGTRAQ
kernel/git/torvalds/linux.git - Linux kernel source tree	
rPath update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Linux Kernel "ptrace_attach()" Privilege Escalation Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
404: File not found	CONFIRM
Linux Kernel 'ptrace_attach()' Local Privilege Escalation Vulnerability	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-05-06	Tomas Hoger	Not vulnerable. This issue did not affect the versions of Linux kernel as shipped with Red Hat E

There are currently no legacy QID mappings associated with this CVE.