CVE-2009-3002

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

Summary

CVE	CVE-2009-3002
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-28 15:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The Linux kernel before 2.6.31-rc7 does not initialize certain data structures within getname functions, which allows local us

Risk And Classification

Primary CVSS: v2.0 4.9 from nvd@nist.gov

AV:L/AC:L/Au:N/C:C/I:N/A:N

Problem Types: CWE-200 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

None

Availability

None

AV:L/AC:L/Au:N/C:C/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.31	-	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc6	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b
Linux Kernel <= 2.6.30 atalk_getname() 8-bytes Stack Disclosure Exploit	af854a3a-2127-422b
RETIRED: Linux Kernel 'net/appletalk/ddp.c' Local Information Disclosure Vulnerability	af854a3a-2127-422b
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b
Ubuntu update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b
oss-security - Re: CVE request: kernel: AF_LLC getsockname 5-Byte Stack Disclosure	af854a3a-2127-422b
519305 – (CVE-2009-3001, CVE-2009-3002) CVE-2009-3001, CVE-2009-3002 kernel: numerous getname() infoleaks	af854a3a-2127-422b
Repository / Oval Repository	af854a3a-2127-422b
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b
git.kernel.org	af854a3a-2127-422b
Repository / Oval Repository	af854a3a-2127-422b
SUSE update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b
USN-852-1: Linux kernel vulnerabilities | Ubuntu	af854a3a-2127-422b
oss-security - Re: CVE request: kernel: AF_LLC getsockname 5-Byte Stack Disclosure	af854a3a-2127-422b
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	af854a3a-2127-422b
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	af854a3a-2127-422b
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	af854a3a-2127-422b

[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	af854a3a-2127-422b
Red Hat Customer Portal	af854a3a-2127-422b
404: File not found	af854a3a-2127-422b
git.kernel.org	af854a3a-2127-422b
About Secunia Research | Flexera	af854a3a-2127-422b
SecurityFocus	af854a3a-2127-422b
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-11-04	Tomas Hoger	CVE-2009-3002 describes a collection of similar information leaks that affect numerous networ

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