



CVE-2008-5079

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

Summary

CVE	CVE-2008-5079
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-12-09 00:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	net/atm/svc.c in the ATM subsystem in the Linux kernel 2.6.27.8 and earlier allows local users to cause a denial of service (

Risk And Classification

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

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

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

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	2.6.20.21	All	All	All
Operating System	Linux	Linux Kernel	2.6.21.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.21.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.21.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.22	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.14	All	All	All

Operating System	Linux	Linux Kernel	2.6.22.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.19	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.20	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.21	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.22	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.22_rc1	All	All	All
Operating System	Linux	Linux Kernel	2.6.22_rc7	All	All	All
Operating System	Linux	Linux Kernel	2.6.23	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.23_rc1	All	All	All
Operating System	Linux	Linux Kernel	2.6.24	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.24_rc1	All	All	All
Operating System	Linux	Linux Kernel	2.6.24_rc4	All	All	All
Operating System	Linux	Linux Kernel	2.6.24_rc5	All	All	All
Operating System	Linux	Linux Kernel	2.6.25	All	All	All

Operating System	Linux	Linux Kernel	2.6.25	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.1	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.10	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.11	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.12	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.2	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.3	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.4	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.5	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.6	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.7	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.8	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.25.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.9	All	x86_64	All
Operating System	Linux	Linux Kernel	2.6.26	All	All	All
Operating System	Linux	Linux Kernel	2.6.26.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.26.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.26.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.26.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.26.5	All	All	All

Operating System	Linux	Linux Kernel	2.6.26.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.27	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference				Source		
Red Hat update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com				af854a3a-2127-422b-91ae-364da266110		
Debian update for linux-2.6.24 - Secunia Advisories - Vulnerability Information - Secunia.com				af854a3a-2127-422b-91ae-364da266110		
Support				af854a3a-2127-422b-91ae-364da266110		
wiki.rpath.com/wiki/Advisories:rPSA-2008-0332				af854a3a-2127-422b-91ae-364da266110		
Red Hat Customer Portal				af854a3a-2127-422b-91ae-364da266110		
Debian -- Security Information -- DSA-1787-1 linux-2.6.24				af854a3a-2127-422b-91ae-364da266110		
Ubuntu update for linux - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-364da266110		
'[PATCH] ATM: CVE-2008-5079: multiple listen()s on same socket corrupts the vcc table' - MARC				af854a3a-2127-422b-91ae-364da266110		
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20				af854a3a-2127-422b-91ae-364da266110		
SecurityFocus				af854a3a-2127-422b-91ae-364da266110		
rPath update for kernel - Secunia.com				af854a3a-2127-422b-91ae-364da266110		
Repository / Oval Repository				af854a3a-2127-422b-91ae-364da266110		
SUSE update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-364da266110		
[SECURITY] Fedora 9 Update: kernel-2.6.27.9-73.fc9				af854a3a-2127-422b-91ae-364da266110		
SUSE update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-364da266110		
Fedora update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-364da266110		
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20				af854a3a-2127-422b-91ae-364da266110		
Ubuntu update for kernel - Secunia.com				af854a3a-2127-422b-91ae-364da266110		
Advisories Mandriva				af854a3a-2127-422b-91ae-364da266110		
SecurityFocus				af854a3a-2127-422b-91ae-364da266110		
Linux Kernel Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-364da266110		
issues.rpath.com/browse/RPL-2915				af854a3a-2127-422b-91ae-364da266110		
Security Advisory SA33623 - Red Hat update for kernel - Secunia				af854a3a-2127-422b-91ae-364da266110		
Linux Kernel svc_listen() Bug Lets Local Users Deny Service - SecurityTracker				af854a3a-2127-422b-91ae-364da266110		
multiple listen()s on same socket corrupts the vcc table - CXSecurity.com				af854a3a-2127-422b-91ae-364da266110		
USN-715-1: Linux kernel vulnerabilities Ubuntu				af854a3a-2127-422b-91ae-364da266110		
USN-714-1: Linux kernel vulnerabilities Ubuntu security notices				af854a3a-2127-422b-91ae-364da266110		

CVE-2009-1471: Linux kernel vulnerabilities Ubuntu security notices	af854a3a-2127-422b-91ae-364da266110
[security-announce] SUSE Security Announcement: Linux kernel (SUSE:2009:	af854a3a-2127-422b-91ae-364da266110
Linux Kernel 'net/atm/proc.c' Local Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da266110
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)