



# CVE-2008-0001

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

## Summary

|                 |                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2008-0001                                                                                                               |
| State           | PUBLISHED                                                                                                                   |
| Assigner        | redhat                                                                                                                      |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                |
| Published       | 2008-01-15 20:00:00 UTC                                                                                                     |
| Updated         | 2026-04-23 00:35:47 UTC                                                                                                     |
| Description     | VFS in the Linux kernel before 2.6.22.16, and 2.6.23.x before 2.6.23.14, performs tests of access mode by using the flag va |

## Risk And Classification

**Primary CVSS:** v2.0 3.6 from nvd@nist.gov

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

**Problem Types:** NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

Partial

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

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product      | Version | Update | Edition | Language |
|------------------|--------|--------------|---------|--------|---------|----------|
| Operating System | Linux  | Linux Kernel | 2.6.0   | All    | All     | All      |

[illegible]

[illegible]



|                  |                       |                              |           |     |     |     |
|------------------|-----------------------|------------------------------|-----------|-----|-----|-----|
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.16.6  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.16.60 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.16.61 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.16.62 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.16.7  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.16.8  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.16.9  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17    | rc1 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17    | rc2 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17    | rc3 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17    | rc4 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17    | rc5 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17    | rc6 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.1  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.10 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.11 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.12 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.13 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.14 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.2  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.3  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.4  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.5  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.6  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.7  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.8  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.17.9  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc1 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc2 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc3 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc4 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc5 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc6 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc7 | All | All |

[illegible]



|                  |                       |                              |                          |                     |                     |                     |
|------------------|-----------------------|------------------------------|--------------------------|---------------------|---------------------|---------------------|
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.23.2</a> | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.23.3</a> | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.23.4</a> | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.23.5</a> | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.23.6</a> | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.23.7</a> | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.23.8</a> | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.23.9</a> | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.3</a>    | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.4</a>    | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.5</a>    | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.6</a>    | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.7</a>    | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.8</a>    | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.8.1</a>  | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.9</a>    | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.9</a>    | <a href="#">rc1</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.9</a>    | <a href="#">rc2</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.9</a>    | <a href="#">rc3</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">2.6.9</a>    | <a href="#">rc4</a> | <a href="#">All</a> | <a href="#">All</a> |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | <a href="#">All</a>      | <a href="#">All</a> | <a href="#">All</a> | <a href="#">All</a> |

| Vendor Declared Affected Products |                    |                     |              |               |  |  |
|-----------------------------------|--------------------|---------------------|--------------|---------------|--|--|
| Source                            | Vendor             | Product             | Version      | Platforms     |  |  |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |  |  |

| References                                                                                |  |  |  |  |                                            |  |
|-------------------------------------------------------------------------------------------|--|--|--|--|--------------------------------------------|--|
| Reference                                                                                 |  |  |  |  | Source                                     |  |
| SUSE update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com    |  |  |  |  | <a href="#">af854a3a-2127-422b-91ae-36</a> |  |
| Ubuntu update for kernel - Advisories - Secunia                                           |  |  |  |  | <a href="#">af854a3a-2127-422b-91ae-36</a> |  |
| Red Hat update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com |  |  |  |  | <a href="#">af854a3a-2127-422b-91ae-36</a> |  |
| <a href="#">issues.rpath.com/browse/RPL-2146</a>                                          |  |  |  |  | <a href="#">af854a3a-2127-422b-91ae-36</a> |  |
| SecurityFocus                                                                             |  |  |  |  | <a href="#">af854a3a-2127-422b-91ae-36</a> |  |
| Debian update for linux-2.6 - Advisories - Secunia                                        |  |  |  |  | <a href="#">af854a3a-2127-422b-91ae-36</a> |  |
| [SECURITY] Fedora 8 Update: kernel-2.6.23.14-107.fc8                                      |  |  |  |  | <a href="#">af854a3a-2127-422b-91ae-36</a> |  |
| rPath update for kernel - Advisories - Secunia                                            |  |  |  |  | <a href="#">af854a3a-2127-422b-91ae-36</a> |  |
| USN-578-1: Linux kernel vulnerabilities   Ubuntu                                          |  |  |  |  | <a href="#">af854a3a-2127-422b-91ae-36</a> |  |

|                                                                                                                 |                            |
|-----------------------------------------------------------------------------------------------------------------|----------------------------|
| USN-574-1: Linux kernel vulnerabilities   Ubuntu                                                                | af854a3a-2127-422b-91ae-36 |
| kernel/git/torvalds/linux.git - Linux kernel source tree                                                        | af854a3a-2127-422b-91ae-36 |
| rhn.redhat.com   Red Hat Support                                                                                | af854a3a-2127-422b-91ae-36 |
| SecurityTracker.com Archives - Linux Kernel VFS Lets Local Users Truncate Directories                           | af854a3a-2127-422b-91ae-36 |
| Advisories   Mandriva                                                                                           | af854a3a-2127-422b-91ae-36 |
| SUSE update for kernel-rt - Advisories - Secunia                                                                | af854a3a-2127-422b-91ae-36 |
| Debian -- Security Information -- DSA-1479-1 linux-2.6                                                          | af854a3a-2127-422b-91ae-36 |
| Linux Kernel VFS Unauthorized File Access Vulnerability                                                         | af854a3a-2127-422b-91ae-36 |
| rhn.redhat.com   Red Hat Support                                                                                | af854a3a-2127-422b-91ae-36 |
| Fedora update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com                        | af854a3a-2127-422b-91ae-36 |
| Red Hat update for kernel - Advisories - Secunia                                                                | af854a3a-2127-422b-91ae-36 |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20                                        | af854a3a-2127-422b-91ae-36 |
| 404: File not found                                                                                             | af854a3a-2127-422b-91ae-36 |
| Ubuntu update for kernel - Advisories - Secunia                                                                 | af854a3a-2127-422b-91ae-36 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                | af854a3a-2127-422b-91ae-36 |
| USN-574-1: Linux kernel vulnerabilities   Ubuntu                                                                | af854a3a-2127-422b-91ae-36 |
| Linux Kernel Directory Truncation Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com | af854a3a-2127-422b-91ae-36 |
| Repository / Oval Repository                                                                                    | af854a3a-2127-422b-91ae-36 |
| Support / Security / Advisories / / MDVSA-2008:112   Mandriva                                                   | af854a3a-2127-422b-91ae-36 |
| 404: File not found                                                                                             | af854a3a-2127-422b-91ae-36 |
| Advisories:rPSA-2008-0021 - rPath Wiki                                                                          | af854a3a-2127-422b-91ae-36 |
| [security-announce] SUSE Security Announcement: Linux kernel security pr                                        | af854a3a-2127-422b-91ae-36 |
| Fedora update for kernel - Advisories - Secunia                                                                 | af854a3a-2127-422b-91ae-36 |
| IBM X-Force Exchange                                                                                            | af854a3a-2127-422b-91ae-36 |
| kernel/git/torvalds/linux.git - Linux kernel source tree                                                        | MITRE                      |
| 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, 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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)