



# CVE-2009-4021

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2009-4021                                                                                                                   |
| <b>State</b>           | PUBLIC                                                                                                                          |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                             |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                    |
| <b>Published</b>       | 2009-11-25 16:30:00 UTC                                                                                                         |
| <b>Updated</b>         | 2023-02-13 02:20:00 UTC                                                                                                         |
| <b>Description</b>     | The fuse_direct_io function in fs/fuse/file.c in the fuse subsystem in the Linux kernel before 2.6.32-rc7 might allow attackers |

## Risk And Classification

### Problem Types: CWE-399

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                | Product                      | Version   | Update | Edition | Language |
|------------------|-----------------------|------------------------------|-----------|--------|---------|----------|
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.0     | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.1     | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.10    | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11    | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.1  | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.10 | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.11 | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.12 | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.2  | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.3  | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.4  | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.5  | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.6  | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.7  | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.8  | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.11.9  | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.12    | All    | All     | All      |

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]



|                  |                       |                              |          |     |     |     |
|------------------|-----------------------|------------------------------|----------|-----|-----|-----|
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.1 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.2 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.3 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.4 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.5 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.6 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.7 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.8 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.9 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc1 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc2 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc3 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc4 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc5 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc6 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc7 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc8 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.1 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.2 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.3 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.4 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.5 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.6 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.32   | rc1 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.32   | rc3 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.32   | rc4 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.32   | rc5 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.4    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.5    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.6    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.7    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.8    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.8.1  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.9    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.0    | All | All | All |

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

|                  |                       |                              |          |     |     |     |
|------------------|-----------------------|------------------------------|----------|-----|-----|-----|
|                  |                       |                              |          |     |     |     |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.28.4 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.28.5 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.28.6 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.28.7 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.28.8 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.28.9 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.29   | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.29.1 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.29.2 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.29.3 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.29.4 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.29.5 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.29.6 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.3    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30   | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.1 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.2 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.3 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.4 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.5 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.6 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.7 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.8 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.30.9 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc1 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc2 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc3 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc4 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc5 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc6 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc7 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31   | rc8 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.1 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.2 | All | All | All |

|                  |                       |                              |          |     |     |     |
|------------------|-----------------------|------------------------------|----------|-----|-----|-----|
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.3 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.4 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.5 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.31.6 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.32   | rc1 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.32   | rc3 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.32   | rc4 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.32   | rc5 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.4    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.5    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.6    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.7    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.8    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.8.1  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.9    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | All      | rc6 | All | All |

| References                                                                                        |  |  |         |  |                                                                                |  |
|---------------------------------------------------------------------------------------------------|--|--|---------|--|--------------------------------------------------------------------------------|--|
| Reference                                                                                         |  |  | Source  |  | Link                                                                           |  |
| Linux Kernel 'fuse_direct_io()' Invalid Pointer Dereference Local Denial of Service Vulnerability |  |  | BID     |  | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20                          |  |  | SUSE    |  | <a href="http://lists.opensuse.org">lists.opensuse.org</a>                     |  |
| oss-security - Re: CVE request: kernel: fuse: prevent fuse_put_request on invalid pointer         |  |  | MLIST   |  | <a href="http://www.openwall.com">www.openwall.com</a>                         |  |
| oss-security - CVE request: kernel: fuse: prevent fuse_put_request on invalid pointer             |  |  | MLIST   |  | <a href="http://www.openwall.com">www.openwall.com</a>                         |  |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20                          |  |  | SUSE    |  | <a href="http://lists.opensuse.org">lists.opensuse.org</a>                     |  |
| rhn.redhat.com   Red Hat Support                                                                  |  |  | REDHAT  |  | <a href="http://rhn.redhat.com">rhn.redhat.com</a>                             |  |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20                          |  |  | SUSE    |  | <a href="http://lists.opensuse.org">lists.opensuse.org</a>                     |  |
| IBM X-Force Exchange                                                                              |  |  | XF      |  | <a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |  |
| kernel/git/torvalds/linux.git - Linux kernel source tree                                          |  |  | MISC    |  | <a href="http://git.kernel.org">git.kernel.org</a>                             |  |
| Debian -- Security Information -- DSA-2005-1 linux-2.6.24                                         |  |  | DEBIAN  |  | <a href="http://www.debian.org">www.debian.org</a>                             |  |
| Red Hat Customer Portal                                                                           |  |  | REDHAT  |  | <a href="http://rhn.redhat.com">rhn.redhat.com</a>                             |  |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20                          |  |  | SUSE    |  | <a href="http://lists.opensuse.org">lists.opensuse.org</a>                     |  |
| SUSE update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com             |  |  | SECUNIA |  | <a href="http://secunia.com">secunia.com</a>                                   |  |
| ASA-2010-026 (RHSA-2010-0046)                                                                     |  |  | CONFIRM |  | <a href="http://support.avaya.com">support.avaya.com</a>                       |  |
| SUSE update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com             |  |  | SECUNIA |  | <a href="http://secunia.com">secunia.com</a>                                   |  |
| kernel/git/torvalds/linux.git - Linux kernel source tree                                          |  |  | CONFIRM |  | <a href="http://git.kernel.org">git.kernel.org</a>                             |  |
| Bug 538734 – CVE-2009-4021 kernel: fuse: prevent fuse_put_request on invalid pointer              |  |  | CONFIRM |  | <a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>                   |  |

|                              |         |                                                               |
|------------------------------|---------|---------------------------------------------------------------|
| Repository / Oval Repository | OVAL    | <a href="https://oval.cisecurity.org">oval.cisecurity.org</a> |
| 404: File not found          | CONFIRM | <a href="https://www.kernel.org">www.kernel.org</a>           |
| Support                      | REDHAT  | <a href="https://www.redhat.com">www.redhat.com</a>           |
| Repository / Oval Repository | OVAL    | <a href="https://oval.cisecurity.org">oval.cisecurity.org</a> |
| CVE Program record           | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                 |
| NVD vulnerability detail     | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>               |

#### Vendor Comments And Credit

| Organization | Published  | Contributor | Statement                                                                                                                                      |
|--------------|------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Red Hat      | 2010-01-21 | Tomas Hoger | Red Hat is aware of this issue and is tracking it via the following bug: <a href="https://bugzilla.redhat.com">https://bugzilla.redhat.com</a> |

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**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)