



# CVE-2009-3725

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

## Summary

|                        |                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2009-3725                                                                                                             |
| <b>State</b>           | PUBLIC                                                                                                                    |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                       |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                              |
| <b>Published</b>       | 2009-11-06 15:30:00 UTC                                                                                                   |
| <b>Updated</b>         | 2018-11-16 15:46:00 UTC                                                                                                   |
| <b>Description</b>     | The connector layer in the Linux kernel before 2.6.31.5 does not require the CAP_SYS_ADMIN capability for certain interac |

## Risk And Classification

### Problem Types: CWE-264

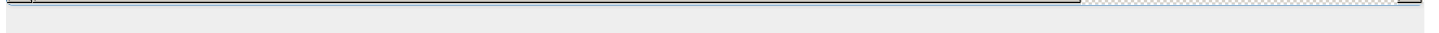
## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                    | Product                      | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 6.06    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 8.04    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 8.10    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 9.04    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 9.10    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 6.06    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 8.04    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 8.10    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 9.04    | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 9.10    | All    | All     | All      |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a> | All     | All    | All     | All      |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a> | All     | All    | All     | All      |

## References

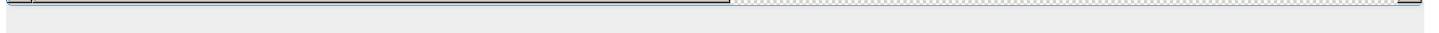
| Reference                                                                             | Source  | Link                                 |
|---------------------------------------------------------------------------------------|---------|--------------------------------------|
| Linux kernel Multiple Capabilities Missing Checks « xorl %eax, %eax                   | MISC    | <a href="#">xorl.wordpress.com</a>   |
| [7/8] pohmelfs/connector: Disallow unpriviled users to configure pohmelfs - Patchwork | CONFIRM | <a href="#">patchwork.kernel.org</a> |

|                                                                                                       |         |                                                                   |
|-------------------------------------------------------------------------------------------------------|---------|-------------------------------------------------------------------|
| 'Re: [oss-security] CVE request: kernel: connector security bypass' - MARC                            | MLIST   | <a href="https://marc.info">marc.info</a>                         |
| USN-864-1: Linux kernel vulnerabilities   Ubuntu                                                      | UBUNTU  | <a href="https://www.ubuntu.com">www.ubuntu.com</a>               |
| [5/8] dm/connector: Only process connector packages from privileged processes - Patchwork             | CONFIRM | <a href="https://patchwork.kernel.org">patchwork.kernel.org</a>   |
| '[oss-security] CVE request: kernel: connector security bypass' - MARC                                | MLIST   | <a href="https://marc.info">marc.info</a>                         |
| 'Re: [PATCH 0/8] SECURITY ISSUE with connector' - MARC                                                | MLIST   | <a href="https://marc.info">marc.info</a>                         |
| 404: File not found                                                                                   | CONFIRM | <a href="https://www.kernel.org">www.kernel.org</a>               |
| Linux Kernel connector Security Bypass - Secunia Advisories - Vulnerability Information - Secunia.com | SECUNIA | <a href="https://secunia.com">secunia.com</a>                     |
| [6/8] dst/connector: Disallow unprivileged users to configure dst - Patchwork                         | CONFIRM | <a href="https://patchwork.kernel.org">patchwork.kernel.org</a>   |
| Debian update for linux-2.6 - Advisories - Community                                                  | SECUNIA | <a href="https://secunia.com">secunia.com</a>                     |
| [8/8] uvesafb/connector: Disallow unprivileged users to send netlink packets - Patchwork              | CONFIRM | <a href="https://patchwork.kernel.org">patchwork.kernel.org</a>   |
| Linux Kernel Subsystem Connector Missing Capability Check Security Bypass Vulnerabilities             | BID     | <a href="https://www.securityfocus.com">www.securityfocus.com</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      | 2009-11-09 | 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.

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

**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)