



# CVE-2010-3861

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

## Summary

|                        |                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2010-3861                                                                                                                    |
| <b>State</b>           | PUBLIC                                                                                                                           |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                              |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                     |
| <b>Published</b>       | 2010-12-10 19:00:00 UTC                                                                                                          |
| <b>Updated</b>         | 2023-02-13 04:27:00 UTC                                                                                                          |
| <b>Description</b>     | The ethtool_get_rxnfc function in net/core/ethtool.c in the Linux kernel before 2.6.36 does not initialize a certain block of he |

## Risk And Classification

### Problem Types: CWE-200

## 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>                         | 10.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>                         | 10.10   | 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>                         | 10.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>                         | 10.10   | 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      |
| Operating System | <a href="#">Opsense</a>   | <a href="#">Opsense</a>                              | 11.2    | All    | All     | All      |
| Operating System | <a href="#">Opsense</a>   | <a href="#">Opsense</a>                              | 11.3    | All    | All     | All      |
| Operating System | <a href="#">Opsense</a>   | <a href="#">Opsense</a>                              | 11.2    | All    | All     | All      |
| Operating System | <a href="#">Opsense</a>   | <a href="#">Opsense</a>                              | 11.3    | All    | All     | All      |
| Operating System | <a href="#">Suse</a>      | <a href="#">Linux Enterprise Desktop</a>             | 11      | sp1    | All     | All      |
| Operating System | <a href="#">Suse</a>      | <a href="#">Linux Enterprise Desktop</a>             | 11      | sp1    | All     | All      |
| Operating System | <a href="#">Suse</a>      | <a href="#">Linux Enterprise Real Time Extension</a> | 11      | sp1    | All     | All      |
| Operating System | <a href="#">Suse</a>      | <a href="#">Linux Enterprise Real Time Extension</a> | 11      | sp1    | All     | All      |
| Operating System | <a href="#">Suse</a>      | <a href="#">Linux Enterprise Server</a>              | 11      | sp1    | All     | All      |

|                                                                                            |      |                         |         |                                                                   |     |     |
|--------------------------------------------------------------------------------------------|------|-------------------------|---------|-------------------------------------------------------------------|-----|-----|
| Operating System                                                                           | Suse | Linux Enterprise Server | 11      | sp1                                                               | All | All |
| References                                                                                 |      |                         |         |                                                                   |     |     |
| Reference                                                                                  |      |                         | Source  | Link                                                              |     |     |
| SUSE update for kernel - Advisories - Community                                            |      |                         | SECUNIA | <a href="https://secunia.com">secunia.com</a>                     |     |     |
| kernel/git/torvalds/linux.git - Linux kernel source tree                                   |      |                         | MISC    | <a href="https://git.kernel.org">git.kernel.org</a>               |     |     |
| [security-announce] SUSE Security Announcement: Realtime Linux Kernel (S                   |      |                         | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>       |     |     |
| access.redhat.com                                                                          |      |                         | REDHAT  | <a href="https://www.redhat.com">www.redhat.com</a>               |     |     |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20                   |      |                         | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>       |     |     |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                           |      |                         | VUPEN   | <a href="https://www.vupen.com">www.vupen.com</a>                 |     |     |
| oss-security - CVE request: kernel: heap contents leak from ETHTOOL_GRXCLSRLALL            |      |                         | MLIST   | <a href="https://openwall.com">openwall.com</a>                   |     |     |
| Linux Kernel ETHTOOL_GRXCLSRLALL Local Information Disclosure Vulnerability                |      |                         | BID     | <a href="https://www.securityfocus.com">www.securityfocus.com</a> |     |     |
| SUSE update for kernel - Advisories - Community                                            |      |                         | SECUNIA | <a href="https://secunia.com">secunia.com</a>                     |     |     |
| kernel/git/torvalds/linux.git - Linux kernel source tree                                   |      |                         | CONFIRM | <a href="https://git.kernel.org">git.kernel.org</a>               |     |     |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20                   |      |                         | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>       |     |     |
| Red Hat update for kernel - Advisories - Community                                         |      |                         | SECUNIA | <a href="https://secunia.com">secunia.com</a>                     |     |     |
| 646725 – (CVE-2010-3861) CVE-2010-3861 kernel: heap contents leak from ETHTOOL_GRXCLSRLALL |      |                         | CONFIRM | <a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>     |     |     |
| 404: File not found                                                                        |      |                         | CONFIRM | <a href="https://www.kernel.org">www.kernel.org</a>               |     |     |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20                   |      |                         | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>       |     |     |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                           |      |                         | VUPEN   | <a href="https://www.vupen.com">www.vupen.com</a>                 |     |     |
| access.redhat.com                                                                          |      |                         | REDHAT  | <a href="https://www.redhat.com">www.redhat.com</a>               |     |     |
| Ubuntu update for linux and linux-ec2 - Advisories - Community                             |      |                         | SECUNIA | <a href="https://secunia.com">secunia.com</a>                     |     |     |
| USN-1041-1: Linux kernel vulnerabilities   Ubuntu                                          |      |                         | UBUNTU  | <a href="https://www.ubuntu.com">www.ubuntu.com</a>               |     |     |
| SUSE update for kernel - Advisories - Community                                            |      |                         | SECUNIA | <a href="https://secunia.com">secunia.com</a>                     |     |     |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                           |      |                         | VUPEN   | <a href="https://www.vupen.com">www.vupen.com</a>                 |     |     |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                           |      |                         | VUPEN   | <a href="https://www.vupen.com">www.vupen.com</a>                 |     |     |
| oss-security - Re: CVE request: kernel: heap contents leak from ETHTOOL_GRXCLSRLALL        |      |                         | MLIST   | <a href="https://openwall.com">openwall.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>                   |     |     |
| No vendor comments have been submitted for this CVE.                                       |      |                         |         |                                                                   |     |     |
| There are currently no legacy QID mappings associated with this CVE.                       |      |                         |         |                                                                   |     |     |

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](https://cve.report/api)

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