



# CVE-2004-0424

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

## Summary

|                 |                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2004-0424                                                                                                                 |
| State           | PUBLISHED                                                                                                                     |
| Assigner        | mitre                                                                                                                         |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                  |
| Published       | 2004-07-07 04:00:00 UTC                                                                                                       |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                       |
| Description     | Integer overflow in the ip_setsockopt function in Linux kernel 2.4.22 through 2.4.25 and 2.6.1 through 2.6.3 allows local use |

## Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

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

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

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product      | Version | Update | Edition | Language |
|------------------|--------|--------------|---------|--------|---------|----------|
| Operating System | Linux  | Linux Kernel | 2.4.22  | All    | All     | All      |

|                  |                           |                                 |            |      |     |     |
|------------------|---------------------------|---------------------------------|------------|------|-----|-----|
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a>    | 2.4.23     | All  | All | All |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a>    | 2.4.23     | pre9 | All | All |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a>    | 2.4.23_ow2 | All  | All | All |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a>    | 2.4.24     | All  | All | All |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a>    | 2.4.24_ow1 | All  | All | All |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a>    | 2.4.25     | 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>    | 2.6.1      | rc1  | All | All |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a>    | 2.6.1      | rc2  | All | All |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a>    | 2.6.2      | All  | All | All |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a>    | 2.6.3      | All  | All | All |
| Application      | <a href="#">Sgi</a>       | <a href="#">Propack</a>         | 3.0        | All  | All | All |
| Operating System | <a href="#">Slackware</a> | <a href="#">Slackware Linux</a> | 9.1        | All  | All | All |
| Operating System | <a href="#">Slackware</a> | <a href="#">Slackware Linux</a> | current    | All  | All | All |

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                               | Link                                |
|------------------------------------------------------------------------------------|--------------------------------------|-------------------------------------|
| Advisories News - LinuxSecurity.com                                                | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.linuxsecurity.</a>  |
| Repository / Oval Repository                                                       | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">oval.cisecurity.org</a> |
| The Slackware Linux Project: Slackware Security Advisories                         | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.slackware.cc</a>    |
| Repository / Oval Repository                                                       | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">oval.cisecurity.org</a> |
| <a href="#">patches.sgi.com/support/free/security/advisories/20040504-01-U.asc</a> | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">patches.sgi.com</a>     |
| <a href="#">www.isec.pl/vulnerabilities/isec-0015-msfilter.txt</a>                 | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.isec.pl</a>         |
| Home - Conectiva                                                                   | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">distro.conectiva.cc</a> |
| <a href="#">redhat.com   Red Hat Support</a>                                       | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.redhat.com</a>      |
| 'Linux kernel setsockopt MCAST_MSFILTER integer overflow' - MARC                   | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">marc.info</a>           |
| Advisories - Mandriva                                                              | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.mandriva.co</a>     |
| Security Announcement                                                              | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.novell.com</a>      |
| Linux Kernel Setsockopt MCAST_MSFILTER Integer Overflow Vulnerability              | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.securityfocus</a>   |
| IBM X-Force Exchange                                                               | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">exchange.xforce.it</a>  |
| CVE Program record                                                                 | CVE.ORG                              | <a href="#">www.cve.org</a>         |
| NVD vulnerability detail                                                           | NVD                                  | <a href="#">nvd.nist.gov</a>        |

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](#)