



# CVE-2005-0180

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

## Summary

|                 |                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2005-0180                                                                                                                                       |
| State           | PUBLISHED                                                                                                                                           |
| Assigner        | mitre                                                                                                                                               |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                                        |
| Published       | 2005-03-07 05:00:00 UTC                                                                                                                             |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                                             |
| Description     | Multiple integer signedness errors in the sg_scsi_ioctl function in scsi_ioctl.c for Linux 2.6.x allow local users to read or modify kernel memory. |

## Risk And Classification

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

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

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

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

## 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      |

|                  |       |              |          |        |     |     |
|------------------|-------|--------------|----------|--------|-----|-----|
| Operating System | Linux | Linux Kernel | 2.6.0    | test1  | All | All |
| Operating System | Linux | Linux Kernel | 2.6.0    | test10 | All | All |
| Operating System | Linux | Linux Kernel | 2.6.0    | test11 | All | All |
| Operating System | Linux | Linux Kernel | 2.6.0    | test2  | All | All |
| Operating System | Linux | Linux Kernel | 2.6.0    | test3  | All | All |
| Operating System | Linux | Linux Kernel | 2.6.0    | test4  | All | All |
| Operating System | Linux | Linux Kernel | 2.6.0    | test5  | All | All |
| Operating System | Linux | Linux Kernel | 2.6.0    | test6  | All | All |
| Operating System | Linux | Linux Kernel | 2.6.0    | test7  | All | All |
| Operating System | Linux | Linux Kernel | 2.6.0    | test8  | All | All |
| Operating System | Linux | Linux Kernel | 2.6.0    | test9  | All | All |
| Operating System | Linux | Linux Kernel | 2.6.1    | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.1    | rc1    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.1    | rc2    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.10   | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.10   | rc2    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11   | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11   | rc2    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11   | rc3    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11   | rc4    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11.1 | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11.2 | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11.3 | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11.4 | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11.5 | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11.6 | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11.7 | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.11.8 | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.12   | rc1    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.12   | rc4    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.2    | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.3    | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.4    | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.5    | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.6    | All    | All | All |
| Operating System | Linux | Linux Kernel | 2.6.6    | rc1    | 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> | 2.6.7         | rc1    | 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         | rc1    | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.8         | rc2    | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.8         | rc3    | 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         | 2.6.20 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6_test9_cvs | All    | All | All |

| Vendor Declared Affected Products |        |         |              |               |  |  |
|-----------------------------------|--------|---------|--------------|---------------|--|--|
| Source                            | Vendor | Product | Version      | Platforms     |  |  |
| CNA                               | Na     | N/a     | affected n/a | Not specified |  |  |

| References                                                             |  |  |                                      |  |                                         |  |
|------------------------------------------------------------------------|--|--|--------------------------------------|--|-----------------------------------------|--|
| Reference                                                              |  |  | Source                               |  | Link                                    |  |
| [Full-Disclosure] grsecurity 2.1.0 release / 5 Linux kernel advisories |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">lists.grok.org.uk</a>       |  |
| SecurityFocus                                                          |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">www.securityfocus.com</a>   |  |
| Advisories - Mandriva Linux                                            |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">www.mandriva.com</a>        |  |
| Secunia - Advisories - Mandriva update for kernel                      |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">secunia.com</a>             |  |
| Home - Conectiva                                                       |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">distro.conectiva.com.br</a> |  |
| Repository / Oval Repository                                           |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">oval.cisecurity.org</a>     |  |
| rhn.redhat.com   Red Hat Support                                       |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">www.redhat.com</a>          |  |
| Linux Kernel SCSI IOCTL Integer Overflow Vulnerability                 |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">www.securityfocus.com</a>   |  |
| Advisories - Mandriva Linux                                            |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">www.mandriva.com</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.

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)