# CVE-2012-0879

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2012-0879 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2012-05-17 11:00:00 UTC |
| **Updated** | 2023-02-13 00:23:00 UTC |
| **Description** | The I/O implementation for block devices in the Linux kernel before 2.6.33 does not properly handle the CLONE_IO feature |

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 10.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 10.04 | All | All | All |
| Operating System | Debian | Debian Linux | 6.0 | All | All | All |
| Operating System | Debian | Debian Linux | 6.0 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Suse | Linux Enterprise Desktop | 11 | sp1 | All | All |
| Operating System | Suse | Linux Enterprise Desktop | 11 | sp2 | All | All |
| Operating System | Suse | Linux Enterprise Desktop | 11 | sp1 | All | All |
| Operating System | Suse | Linux Enterprise Desktop | 11 | sp2 | All | All |
| Operating System | Suse | Linux Enterprise High Availability Extension | 11 | sp1 | All | All |
| Operating System | Suse | Linux Enterprise High Availability Extension | 11 | sp1 | All | All |
| Operating System | Suse | Linux Enterprise Server | 11 | sp1 | All | All |
| Operating System | Suse | Linux Enterprise Server | 11 | sp1 | All | All |
| Operating System | Suse | Linux Enterprise Server | 11 | sp2 | All | All |
| Operating System | Suse | Linux Enterprise Server | 11 | sp1 | All | All |
| Operating System | Suse | Linux Enterprise Server | 11 | sp1 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Suse | Linux Enterprise Server | 11 | sp2 | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| USN-1410-1: Linux kernel (EC2) vulnerability \| Ubuntu | UBUNTU | www.ubu |
| kernel/git/torvalds/linux.git - Linux kernel source tree | CONFIRM | git.kernel |
| Red Hat Customer Portal | REDHAT | rhn.redha |
| kernel/git/torvalds/linux.git - Linux kernel source tree | CONFIRM | git.kernel |
| Security Advisory SA48545 - Ubuntu update for linux - Secunia | SECUNIA | secunia.c |
| kernel/git/torvalds/linux.git - Linux kernel source tree | MISC | git.kernel |
| USN-1411-1: Linux kernel vulnerability \| Ubuntu | UBUNTU | www.ubu |
| block: Fix io_context leak after clone with CLONE_IO · torvalds/linux@61cc74f · GitHub | CONFIRM | github.co |
| '[security bulletin] HPSBGN02970 rev.1 - HP Rapid Deployment Pack (RDP) or HP Insight Control Server ' - MARC | HP | marc.info |
| Linux Kernel CLONE_IO Bug Lets Local Users Deny Service - SecurityTracker | SECTRACK | www.sec |
| block: Fix io_context leak after failure of clone with CLONE_IO · torvalds/linux@b69f229 · GitHub | CONFIRM | github.co |
| Debian -- Security Information -- DSA-2469-1 linux-2.6 | DEBIAN | www.deb |
| RHSA-2012:0481 | REDHAT | rhn.redha |
| Bug 796829 – CVE-2012-0879 kernel: block: CLONE_IO io_context refcounting issues | CONFIRM | bugzilla.r |
| About Secunia Research \| Flexera | SECUNIA | secunia.c |
| oss-security - Re: CVE request -- kernel: block: CLONE_IO io_context refcounting issues | MLIST | www.ope |
| USN-1408-1: Linux kernel (FSL-IMX51) vulnerability \| Ubuntu | UBUNTU | www.ubu |
| 404 Not Found | CONFIRM | ftp.osuos |
| git.kernel.org | MISC | git.kernel |
| [security-announce] SUSE-SU-2012:0616-1: important: Security update for | SUSE | lists.oper |
| CVE Program record | CVE.ORG | www.cve |
| NVD vulnerability detail | NVD | nvd.nist.g |

No vendor comments have been submitted for this CVE.

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

**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**