



# CVE-2011-3637

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

## Summary

|                 |                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2011-3637                                                                                                               |
| State           | PUBLISHED                                                                                                                   |
| Assigner        | redhat                                                                                                                      |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                |
| Published       | 2012-05-17 11:00:31 UTC                                                                                                     |
| Updated         | 2026-04-29 01:13:23 UTC                                                                                                     |
| Description     | The m_stop function in fs/proc/task_mmu.c in the Linux kernel before 2.6.39 allows local users to cause a denial of service |

## Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-476 | n/a

| Version | Source       | Type    | Score | Severity | Vector                                       |
|---------|--------------|---------|-------|----------|----------------------------------------------|
| 3.1     | nvd@nist.gov | Primary | 5.5   | MEDIUM   | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H |
| 2.0     | nvd@nist.gov | Primary | 4.9   |          | AV:L/AC:L/Au:N/C:N/I:N/A:C                   |

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

#### CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

#### NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product          | Version | Update | Edition | Language |
|------------------|--------|------------------|---------|--------|---------|----------|
| Operating System | Linux  | Linux Kernel     | All     | All    | All     | All      |
| Operating System | Redhat | Enterprise Linux | 6.0     | All    | All     | All      |

#### Vendor Declared Affected Products

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

#### References

| Reference                                                                                    | Source                               |
|----------------------------------------------------------------------------------------------|--------------------------------------|
| proc: fix oops on invalid /proc/<pid>/maps access · torvalds/linux@76597cd · GitHub          | af854a3a-2127-422b-91ae-364da2661108 |
| oss-security - CVE-2011-3637 Linux kernel: proc: fix Oops on invalid /proc/<pid>/maps access | af854a3a-2127-422b-91ae-364da2661108 |
| Bug 747848 – CVE-2011-3637 kernel: proc: fix oops on invalid /proc/<pid>/maps access         | af854a3a-2127-422b-91ae-364da2661108 |
| 404 Not Found                                                                                | af854a3a-2127-422b-91ae-364da2661108 |
| kernel/git/torvalds/linux.git - Linux kernel source tree                                     | af854a3a-2127-422b-91ae-364da2661108 |
| kernel/git/torvalds/linux.git - Linux kernel source tree                                     | MITRE                                |
| CVE Program record                                                                           | CVE.ORG                              |
| NVD vulnerability detail                                                                     | NVD                                  |

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](#)