



Published on: 09/30/2005 12:00:00 AM UTC

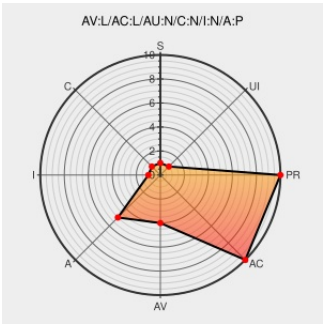
Last Modified on: 03/23/2021 11:27:23 PM UTC

# CVE-2005-3107

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

fs/exec.c in Linux 2.6, when one thread is tracing another thread that shares the same memory map, might allow local users to cause a denial of service (deadlock) by forcing a core dump when the traced thread is in the TASK\_TRACED state.

CVE-2005-3107 has been assigned by [M cve@mitre.org](mailto:m_cve@mitre.org) to track the vulnerability

CVSS2 Score: 2.1 - LOW

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| LOCAL                  | LOW               | NONE                |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| NONE                   | NONE              | PARTIAL             |

## CVE References

| Description                                      | Tags                                                                                   | Link                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secunia - Advisories - Ubuntu update for kernel  | <a href="#">web.archive.org</a><br><a href="#">text/html</a>                           |  SECUNIA 17141                                                                                                                                                                                                                                                                                                                                     |
|                                                  | <a href="#">Patch</a><br><a href="#">www.kernel.org</a><br><a href="#">text/x-diff</a> |  CONFIRM<br><a href="http://www.kernel.org/pub/linux/kernel/people/akpm/patches/2.6/2.6.11-rc1/2.6.11-rc1-mm1/broken-out/fix-coredump_wait-deadlock-with-pttracee-on-shared-mm.patch">www.kernel.org/pub/linux/kernel/people/akpm/patches/2.6/2.6.11-rc1/2.6.11-rc1-mm1/broken-out/fix-coredump_wait-deadlock-with-pttracee-on-shared-mm.patch</a> |
| Advisories - Mandriva                            | <a href="#">www.mandriva.com</a><br><a href="#">text/html</a>                          |  MANDRIVA MDKSA-2006:072                                                                                                                                                                                                                                                                                                                           |
| Red Hat update for kernel - Advisories - Secunia | <a href="#">web.archive.org</a><br><a href="#">text/html</a>                           |  SECUNIA 21136                                                                                                                                                                                                                                                                                                                                     |
| ASA-2006-180 (RHSA-2006-0437)                    | <a href="#">support.avaya.com</a><br><a href="#">text/html</a>                         |  CONFIRM <a href="http://support.avaya.com/elmodocs2/security/ASA-2006-180.htm">support.avaya.com/elmodocs2/security/ASA-2006-180.htm</a>                                                                                                                                                                                                          |

|                                                                                   |                                                |                                                                                                            |
|-----------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| No Description Provided                                                           | Broken Link<br>linux.bkbits.net                | CONFIRM linux.bkbits.net:8080/linux-2.6/diffs/fs/exec.c@1.155?<br>nav=index.html src src/fs hist/fs/exec.c |
|                                                                                   | Inactive Link Not Archived                     |                                                                                                            |
| rhn.redhat.com   Red Hat Support                                                  | www.redhat.com<br>text/html                    | REDHAT RHSA-2006:0437                                                                                      |
| usn.usn-199-1 - Ubuntu Linux                                                      | www.ubuntu.com<br>text/html                    | UBUNTU USN-199-1                                                                                           |
| Debian -- Security Information --<br>DSA-922-1 kernel-source-2.6.8                | www.debian.org<br>Deprecated Link<br>text/html | DEBIAN DSA-922                                                                                             |
| Linux Kernel Multiple Security<br>Vulnerabilities                                 | cve.report (archive)<br>text/html              | BID 15049                                                                                                  |
| Support                                                                           | www.redhat.com<br>text/html                    | REDHAT RHSA-2005:420                                                                                       |
| Repository / Oval Repository                                                      | oval.cisecurity.org<br>text/html               | OVAL oval:org.mitre.oval:def:11473                                                                         |
| Avaya Products Linux Kernel<br>Multiple Vulnerabilities - Advisories<br>- Secunia | web.archive.org<br>text/html                   | SECUNIA 21983                                                                                              |
| Secunia - Advisories - Debian<br>update for kernel-source-2.6.8                   | web.archive.org<br>text/html                   | SECUNIA 18056                                                                                              |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| 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   | All    | All     | All      |
| cpe:2.3:o:linux:linux_kernel:2.6.0:*****:.* |        |              |         |        |         |          |
| cpe:2.3:o:linux:linux_kernel:2.6.0:*****:.* |        |              |         |        |         |          |

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)