



# CVE-2011-1745

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2011-1745                                                                                                                |
| <b>State</b>           | PUBLIC                                                                                                                       |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                          |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                 |
| <b>Published</b>       | 2011-05-09 19:55:00 UTC                                                                                                      |
| <b>Updated</b>         | 2023-02-13 00:17:00 UTC                                                                                                      |
| <b>Description</b>     | Integer overflow in the agp_generic_insert_memory function in drivers/char/agp/generic.c in the Linux kernel before 2.6.38.1 |

## Risk And Classification

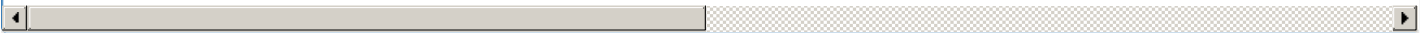
### Problem Types: CWE-190

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                                      | Version | Update | Edition | Language |
|------------------|------------------------|----------------------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a>                 | All     | All    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a>                 | All     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux</a>             | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux</a>             | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Aus</a>         | 5.6     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Aus</a>         | 5.6     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Desktop</a>     | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Desktop</a>     | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Eus</a>         | 5.6     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Eus</a>         | 5.6     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 5.0     | All    | All     | All      |

## References

### Reference

|                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">access.redhat.com</a>                                                                                                  |
| oss-security - CVE request: kernel: buffer overflow and DoS issues in agp                                                          |
| Linux Kernel 'agp_ioctl()' Local Privilege Escalation Vulnerability                                                                |
| <a href="#">git.kernel.org</a>                                                                                                     |
| <a href="#">kernel/git/torvalds/linux.git</a> - Linux kernel source tree                                                           |
| 698996 – (CVE-2011-1745, CVE-2011-2022) CVE-2011-1745 CVE-2011-2022 kernel: agp: insufficient pg_start parameter checking in AGPIC |
| LKML: Vasily Kulikov: [PATCH] char: agp: fix arbitrary kernel memory writes                                                        |
| oss-security - Re: CVE request: kernel: buffer overflow and DoS issues in agp                                                      |
| 404: File not found                                                                                                                |
| CVE Program record                                                                                                                 |
| NVD vulnerability detail                                                                                                           |
|                                                   |
| 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](#)