CVE-2011-1745

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

Summary

CVE	CVE-2011-1745
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-09 19:55:00 UTC
Updated	2023-02-13 00:17:00 UTC
Description	Integer overflow in the agp_generic_insert_memory function in drivers/char/agp/generic.c in the Linux kernel before 2.6.38.

Risk And Classification

Problem Types: CWE-190

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	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Aus	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Aus	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All

References

Reference

access.redhat.com
oss-security - CVE request: kernel: buffer overflow and DoS issues in agp
Linux Kernel 'agp_ioctl()' Local Privilege Escalation Vulnerability
git.kernel.org
kernel/git/torvalds/linux.git - 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: Vasiliy 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.