CVE-2011-0521

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

Summary

CVE	CVE-2011-0521
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-02 23:00:32 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The dvb_ca_ioctl function in drivers/media/dvb/ttpci/av7110_ca.c in the Linux kernel before 2.6.38-rc2 does not check the s

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/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	Linux	Linux Kernel	2.6.38	-	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc1	All	All

Vendor Declared Affected Products

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

References

Reference	Source
oss-security - Re: Linux kernel av7110 negative array offset	af854a3a-2127-422b-
404: File not found	af854a3a-2127-422b-
oss-security - Linux kernel av7110 negative array offset	af854a3a-2127-422b-
SecurityFocus	af854a3a-2127-422b-
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-
About Secunia Research | Flexera	af854a3a-2127-422b-
VMSA-2011-0012.2	af854a3a-2127-422b-
IBM X-Force Exchange	af854a3a-2127-422b-
Linux Kernel Multiple Vulnerabilities - Secunia.com	af854a3a-2127-422b-
Linux Kernel 'drivers/media/dvb/ttpci/av7110_ca' IOCTL Local Privilege Escalation Vulnerability	af854a3a-2127-422b-
Linux Kernel AV7110 Driver dvb_ca_ioctl() Memory Corruption Error Lets Local Users Deny Service - SecurityTracker	af854a3a-2127-422b-
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.