



CVE-2010-1083

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

Summary

CVE	CVE-2010-1083
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-04-06 22:30:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The processcompl_compat function in drivers/usb/core/devio.c in Linux kernel 2.6.x through 2.6.32, and possibly other vers

Risk And Classification

Primary CVSS: v2.0 4.7 from nvd@nist.gov

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

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.0	All	All	All

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Operating System	Linux	Linux Kernel	2.6.28.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.29	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.30	All	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc7-git6	All	All
Operating System	Linux	Linux Kernel	2.6.30.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.31	All	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc8	All	All
Operating System	Linux	Linux Kernel	2.6.31.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.10	All	All	All

Operating System	Linux	Linux Kernel	2.6.31.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

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

References						
Reference				Source	Link	
SUSE update for kernel - Secunia.com				af854a3a-2127-422b-91ae-364da2661108	secunia	
[80/93] USB: usbfs: properly clean up the as structure on error paths [LWN.net]				af854a3a-2127-422b-91ae-364da2661108	lwn.net	
Support				af854a3a-2127-422b-91ae-364da2661108	www.red	
ASA-2010-146 (RHSA-2010-0394 RHSA-2010-0424)				af854a3a-2127-422b-91ae-364da2661108	support.	
oss-security - Re: CVE request: kernel information leak via userspace USB interface				af854a3a-2127-422b-91ae-364da2661108	www.op	
Security Announcement				af854a3a-2127-422b-91ae-364da2661108	www.no	
SecurityFocus				af854a3a-2127-422b-91ae-364da2661108	www.se	
Support				af854a3a-2127-422b-91ae-364da2661108	www.red	
Debian -- Security Information -- DSA-2053-1 linux-2.6				af854a3a-2127-422b-91ae-364da2661108	www.de	
Repository / Oval Repository				af854a3a-2127-422b-91ae-364da2661108	oval.cisc	

oss-security - Re: CVE request: kernel information leak via userspace USB interface	af854a3a-2127-422b-91ae-364da2661108	www.op
About Secunia Research Flexera	af854a3a-2127-422b-91ae-364da2661108	secunia
VMSA-2011-0012.2	af854a3a-2127-422b-91ae-364da2661108	www.vr
Debian update for linux-2.6 - Advisories - Community	af854a3a-2127-422b-91ae-364da2661108	secunia
oss-security - Re: additional memory leak in USB userspace handling	af854a3a-2127-422b-91ae-364da2661108	www.op
LKML: Greg KH: [48/89] USB: usbfs: properly clean up the as structure on error paths	af854a3a-2127-422b-91ae-364da2661108	lkml.org
oss-security - CVE request: kernel information leak via userspace USB interface	af854a3a-2127-422b-91ae-364da2661108	www.op
oss-security - additional memory leak in USB userspace handling	af854a3a-2127-422b-91ae-364da2661108	www.op
ASA-2010-291 (RHSA-2010-0723)	af854a3a-2127-422b-91ae-364da2661108	support.
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	af854a3a-2127-422b-91ae-364da2661108	lists.ope
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-04-07	Vincent Danen	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.co

There are currently no legacy QID mappings associated with this CVE.