



# CVE-2016-4482

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

## Summary

<b>CVE</b>	CVE-2016-4482
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-05-23 10:59:00 UTC
<b>Updated</b>	2023-09-12 14:55:00 UTC
<b>Description</b>	The proc_connectinfo function in drivers/usb/core/devio.c in the Linux kernel through 4.6 does not initialize a certain data st

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Debuginfo</a>	11.0	sp4	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Debuginfo</a>	11.0	sp4	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Desktop</a>	12.0	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Desktop</a>	12.0	sp1	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Desktop</a>	12.0	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Desktop</a>	12.0	sp1	All	All

Operating System	Novell	Suse Linux Enterprise Live Patching	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Live Patching	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Module For Public Cloud	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Module For Public Cloud	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Real Time Extension	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Real Time Extension	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	extra	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	extra	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	sp1	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp4	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	sp1	All	All

## References

Reference	Source	Link	Tags
USN-3018-2: Linux kernel (Trusty HWE) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
USN-3016-3: Linux kernel (Qualcomm Snapdragon) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
USN-3016-1: Linux kernel vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
[security-announce] SUSE-SU-2016:1937-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	Third Party Advisory
[security-announce] openSUSE-SU-2016:1641-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	

Linux Kernel CVE-2016-4482 Local Information Disclosure vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
USN-3017-3: Linux kernel (Wily HWE) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
oss-security - CVE Request: information leak in devio of Linux kernel	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
[SECURITY] Fedora 24 Update: kernel-4.5.3-300.fc24	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[security-announce] SUSE-SU-2016:1985-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	<a href="http://git.kernel.org">git.kernel.org</a>	Vendor Advisory
USN-3021-2: Linux kernel (OMAP4) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
USN-3017-1: Linux kernel vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
USN-3017-2: Linux kernel (Raspberry Pi 2) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
USN-3016-4: Linux kernel (Xenial HWE) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
USN-3021-1: Linux kernel vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
[security-announce] SUSE-SU-2016:1672-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	Third Party Advisory
USN-3019-1: Linux kernel (Utopic HWE) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
Debian -- Security Information -- DSA-3607-1 linux	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
USB: usbfs: fix potential infoleak in devio · torvalds/linux@681fef8 · GitHub	CONFIRM	<a href="http://github.com">github.com</a>	Vendor Advisory
USN-3020-1: Linux kernel (Vivid HWE) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
USN-3016-2: Linux kernel (Raspberry Pi 2) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
[security-announce] SUSE-SU-2016:1690-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	Third Party Advisory
[security-announce] SUSE-SU-2016:2105-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
[security-announce] SUSE-SU-2016:1696-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	Third Party Advisory
[security-announce] openSUSE-SU-2016:2184-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
USN-3018-1: Linux kernel vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
1332931 – (CVE-2016-4482) CVE-2016-4482 kernel: information leak in devio.c	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tracking
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org). This site includes MITRE data granted under the following [license](http://www.mitre.org).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)