



# CVE-2016-3951

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

## Summary

<b>CVE</b>	CVE-2016-3951
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-05-02 10:59:00 UTC
<b>Updated</b>	2017-08-13 01:29:00 UTC
<b>Description</b>	Double free vulnerability in drivers/net/usb/cdc_ncm.c in the Linux kernel before 4.5 allows physically proximate attackers to

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## 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>	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="#">Linux</a>	<a href="#">Linux Kernel</a>	4.5.0	rc7	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	4.5.0	rc7	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Desktop</a>	12	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Desktop</a>	12	sp1	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Desktop</a>	12	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Desktop</a>	12	sp1	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Live Patching</a>	12.0	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Live Patching</a>	12.0	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Module For Public Cloud</a>	12	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Module For Public Cloud</a>	12	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Real Time Extension</a>	12	sp1	All	All

Operating System	Novell	<a href="#">Suse Linux Enterprise Real Time Extension</a>	12	sp1	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Server</a>	12.0	All	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Server</a>	12.0	sp1	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Server</a>	12.0	All	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Server</a>	12.0	sp1	All	All
Application	Novell	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12.0	sp1	All	All
Application	Novell	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12.0	sp1	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Workstation Extension</a>	12.0	All	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Workstation Extension</a>	12.0	sp1	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Workstation Extension</a>	12.0	All	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Workstation Extension</a>	12.0	sp1	All	All
Application	Suse	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12.0	All	All	All
Application	Suse	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12.0	All	All	All

## References

### Reference

[security-announce] openSUSE-SU-2016:1382-1: important: Security update

[kernel/git/torvalds/linux.git](#) - Linux kernel source tree

1324782 – (CVE-2016-3951) CVE-2016-3951 kernel: crash on invalid USB device descriptors (usbnet driver)

USN-3000-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu

Linux Kernel CVE-2016-3951 Null Pointer Deference Local Denial of Service Vulnerability

Google Android Multiple Flaws Let Remote Users Deny Service and Execute Arbitrary Code and Let Applications Obtain Potentially Sensitive

USN-2998-1: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu

USN-3021-2: Linux kernel (OMAP4) vulnerabilities | Ubuntu

USN-3001-1: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu

USN-3004-1: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu

[kernel/git/torvalds/linux.git](#) - Linux kernel source tree

USN-3021-1: Linux kernel vulnerabilities | Ubuntu

USN-3002-1: Linux kernel (Wily HWE) vulnerabilities | Ubuntu

usbnet: cleanup after bind() in probe() · torvalds/linux@1666984 · GitHub

Debian -- Security Information -- DSA-3607-1 linux

[security-announce] SUSE-SU-2016:1764-1: important: Security update for

USN-2989-1: Linux kernel vulnerabilities | Ubuntu

USN-3003-1: Linux kernel vulnerabilities | Ubuntu

Re: Possible double-free in the usbnet driver — Linux Network Development

[security-announce] openSUSE-SU-2016:1382-1: important: Security update

[security-announce] SUSE-SU-2016:1690-1: important: Security update for

[security-announce] SUSE-SU-2016:1696-1: important: Security update for

oss-security - Fwd: CVE Request: Linux: usbnet: memory corruption triggered by invalid USB descriptor

cdc\_ncm: do not call usbnet\_link\_change from cdc\_ncm\_bind · torvalds/linux@4d06dd5 · GitHub

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**