



# CVE-2016-4486

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

## Summary

<b>CVE</b>	CVE-2016-4486
<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 rtnl_fill_link_ifmap function in net/core/rtnetlink.c in the Linux kernel before 4.5.5 does not initialize a certain data struct

## Risk And Classification

### Problem Types: CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Debuginfo	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Debuginfo	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	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	<a href="#">Suse Linux Enterprise Module For Public Cloud</a>	12.0	All	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Module For Public Cloud</a>	12.0	All	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Real Time Extension</a>	12.0	sp1	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Real Time Extension</a>	12.0	sp1	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Server</a>	11.0	extra	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Server</a>	11.0	sp4	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>	11.0	extra	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Server</a>	11.0	sp4	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>	11.0	sp4	All	All
Application	Novell	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12.0	All	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 Software Development Kit</a>	11.0	sp4	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12.0	All	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12.0	sp1	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Software Development Kit</a>	11.0	sp4	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12.0	All	All	All
Operating System	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

## References

Reference	Source	Link	Tags
USN-3005-1: Linux kernel (Xenial HWE) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv
[security-announce] SUSE-SU-2016:1937-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	Third Party Adv
[security-announce] openSUSE-SU-2016:1641-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
USN-3000-1: Linux kernel (Utopic HWE) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv
Linux Kernel 4.4 - 'rtnetlink' Stack Memory Disclosure - Linux local Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	
[security-announce] SUSE-SU-2016:1985-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
USN-2998-1: Linux kernel (Trusty HWE) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv

oss-security - CVE Request: kernel information leak vulnerability in rtnetlink	MLIS I	<a href="http://www.openwall.com">www.openwall.com</a>	
USN-3001-1: Linux kernel (Vivid HWE) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv
USN-3004-1: Linux kernel (Raspberry Pi 2) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv
1333316 – (CVE-2016-4486) CVE-2016-4486 kernel: Information leak in rtnetlink	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tracking,
USN-3007-1: Linux kernel (Raspberry Pi 2) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv
net: fix infoleak in rtnetlink · torvalds/linux@5f8e447 · GitHub	CONFIRM	<a href="http://github.com">github.com</a>	Vendor Advisor
[security-announce] SUSE-SU-2016:2074-1: 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>	
[security-announce] SUSE-SU-2016:1672-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	Third Party Adv
USN-3002-1: Linux kernel (Wily HWE) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv
Debian -- Security Information -- DSA-3607-1 linux	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
<a href="http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.5">www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.5</a>	CONFIRM	<a href="http://www.kernel.org">www.kernel.org</a>	
USN-2996-1: Linux kernel vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv
USN-2989-1: Linux kernel vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv
USN-3003-1: Linux kernel vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv
USN-3006-1: Linux kernel vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv
[security-announce] SUSE-SU-2016:1690-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	Third Party Adv
[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 Adv
[security-announce] openSUSE-SU-2016:2184-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
USN-2997-1: Linux kernel (OMAP4) vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Adv
Linux Kernel CVE-2016-4486 Local Information Disclosure Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
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, analy

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

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

