



# CVE-2016-4805

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2016-4805
<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>	2023-01-17 21:18:00 UTC
<b>Description</b>	Use-after-free vulnerability in drivers/net/ppp/ppp_generic.c in the Linux kernel before 4.5.2 allows local users to cause a de

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Novell	Opensuse Leap	42.1	All	All	All
Operating System	Novell	Opensuse Leap	42.1	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	-	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
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp1	All	All
Application	Novell	Suse Linux Enterprise Live Patching	12.0	-	All	All
Application	Novell	Suse Linux Enterprise Live Patching	12.0	-	All	All
Application	Novell	Suse Linux Enterprise Module For Public Cloud	12.0	-	All	All
Application	Novell	Suse Linux Enterprise Module For Public Cloud	12.0	-	All	All
Operating System	Novell	Suse Linux Enterprise Real Time Extension	11.0	sp4	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	11.0	sp4	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	sp4	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Server</a>	12.0	-	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	sp4	All	All
Operating System	Novell	<a href="#">Suse Linux Enterprise Server</a>	12.0	-	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
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>	11.0	sp4	All	All
Application	Novell	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12.0	-	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 Workstation Extension</a>	12.0	-	All	All
Application	Novell	<a href="#">Suse Linux Enterprise Workstation Extension</a>	12.0	sp1	All	All
Application	Novell	<a href="#">Suse Linux Enterprise Workstation Extension</a>	12.0	-	All	All
Application	Novell	<a href="#">Suse Linux Enterprise Workstation Extension</a>	12.0	sp1	All	All
Operating System	Oracle	<a href="#">Linux</a>	6	All	All	All
Operating System	Oracle	<a href="#">Linux</a>	6	All	All	All
Operating System	Redhat	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	Redhat	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	Redhat	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	Redhat	<a href="#">Enterprise Linux</a>	7.0	All	All	All

## References

### Reference

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

[ppp: take reference on channels netns · torvalds/linux@1f461dc · GitHub](#)

[Linux kernel 'ppp\\_generic.c' Use After Free Denial of Service Vulnerability](#)

[\[security-announce\] SUSE-SU-2016:1937-1: important: Security update for](#)

[\[security-announce\] openSUSE-SU-2016:1641-1: important: Security update](#)

[Oracle Linux Bulletin - July 2016](#)

[\[security-announce\] SUSE-SU-2016:1985-1: important: Security update for](#)

[Google Android Multiple Flaws Let Remote Users Deny Service and Execute Arbitrary Code and Let Applications Obtain Potentially Sensitive](#)

[USN-3021-2: Linux kernel \(OMAP4\) vulnerabilities | Ubuntu](#)

oss-security - Re: CVE Requests: Linux: use-atter-tree issue for ppp channel

[www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.2](http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.2)

USN-3021-1: Linux kernel vulnerabilities | Ubuntu

[security-announce] SUSE-SU-2016:1672-1: important: Security update for

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

Oracle VM Server for x86 Bulletin - October 2016

1335803 – (CVE-2016-4805) CVE-2016-4805 kernel: Use after free vulnerability in ppp\_unregister\_channel

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

[security-announce] SUSE-SU-2016:2105-1: important: Security update for

[security-announce] openSUSE-SU-2016:2184-1: important: Security update

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

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

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