



# CVE-2016-5244

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2016-5244
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-06-27 10:59:00 UTC
<b>Updated</b>	2019-04-22 17:48:00 UTC
<b>Description</b>	The rds_inc_info_copy function in net/rds/recv.c in the Linux kernel through 4.6.3 does not initialize a certain structure mem

## 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="#">Fedoraproject</a>	<a href="#">Fedora</a>	22	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	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>	22	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	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="#">Redhat</a>	<a href="#">Enterprise Linux</a>	5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Linux Enterprise Debuginfo</a>	11	sp4	All	All
Application	<a href="#">Suse</a>	<a href="#">Linux Enterprise Debuginfo</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Real Time Extension</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Real Time Extension</a>	12	sp1	All	All

Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Real Time Extension</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Real Time Extension</a>	12	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	extra	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	extra	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Workstation Extension</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Workstation Extension</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Opensuse Leap</a>	42.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Opensuse Leap</a>	42.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Server</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Server</a>	12	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Software Development Kit</a>	11	sp4	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Software Development Kit</a>	11	sp4	All	All
Application	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12	All	All	All

## References

### Reference

USN-3070-2: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu

[security-announce] SUSE-SU-2016:1937-1: important: Security update for

[security-announce] openSUSE-SU-2016:1641-1: important: Security update

[security-announce] SUSE-SU-2016:1985-1: important: Security update for

rds: fix an infoleak in rds\_inc\_info\_copy · torvalds/linux@41116def · GitHub

USN-3070-4: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu

USN-3072-1: Linux kernel vulnerabilities | Ubuntu

USN-3071-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu

USN-3072-2: Linux kernel (OMAP4) vulnerabilities | Ubuntu

USN-3071-1: Linux kernel vulnerabilities | Ubuntu

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

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

Solaris Kernel Multiple Bugs Let Remote and Local Users Access Data, Modify Data, and Deny Service on the Target System - SecurityTrack

Linux Kernel 'net/rds/recv.c' Local Information Disclosure Vulnerability

CPU Oct 2018

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

[security-announce] SUSE-SU-2016:2145-1: important: Security update for

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

USN-3070-1: Linux kernel vulnerabilities | Ubuntu

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

kernel/git/torvalds/linux.git - Linux kernel source tree

USN-3070-3: Linux kernel (Qualcomm Snapdragon) vulnerabilities | Ubuntu

rds: fix an infoleak in rds\_inc\_info\_copy - Patchwork

oss-security - Re: CVE Request: rds: fix an infoleak in rds\_inc\_info\_copy

1343337 – (CVE-2016-5244) CVE-2016-5244 kernel: Information leak in rds\_inc\_info\_copy

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](#)