



CVE-2016-9576

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary	
CVE	CVE-2016-9576
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-28 07:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The blk_rq_map_user_iov function in block/blk-map.c in the Linux kernel before 4.8.14 does not properly restrict the type of

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-416 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown	
Attack Vector	Local
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References	
Reference	Source
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da266110
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-91ae-364da266110
[security-announce] SUSE-SU-2016:3188-1: important: Security update for	af854a3a-2127-422b-91ae-364da266110
[security-announce] SUSE-SU-2016:3217-1: important: Security update for	af854a3a-2127-422b-91ae-364da266110
oss-security - Linux Kernel use-after-free in SCSI generic device interface	af854a3a-2127-422b-91ae-364da266110
[security-announce] SUSE-SU-2016:3248-1: important: Security update for	af854a3a-2127-422b-91ae-364da266110
[security-announce] openSUSE-SU-2016:3086-1: important: Security update	af854a3a-2127-422b-91ae-364da266110
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da266110
[security-announce] SUSE-SU-2016:3203-1: important: Security update for	af854a3a-2127-422b-91ae-364da266110
[security-announce] openSUSE-SU-2016:3085-1: important: Security update	af854a3a-2127-422b-91ae-364da266110

[security-announce] SUSE-SU-2016:3252-1: important: Security update for	af854a3a-2127-422b-91ae-364da266110
[security-announce] SUSE-SU-2016:3146-1: important: Security update for	af854a3a-2127-422b-91ae-364da266110
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.8.14	af854a3a-2127-422b-91ae-364da266110
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da266110
Bug 1403145 – CVE-2016-9576 kernel: Use after free in SCSI generic device interface	af854a3a-2127-422b-91ae-364da266110
Don't feed anything but regular iovec's to blk_rq_map_user_iov · torvalds/linux@a0ac402 · GitHub	af854a3a-2127-422b-91ae-364da266110
Linux Kernel CVE-2016-9576 Use After Free Memory Corruption Vulnerability	af854a3a-2127-422b-91ae-364da266110
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da266110
[security-announce] openSUSE-SU-2016:3118-1: important: Security update	af854a3a-2127-422b-91ae-364da266110
Red Hat Customer Portal	MITRE
CVE-2016-9576 - Red Hat Customer Portal	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

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

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