CVE-2016-4565

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

Summary

CVE	CVE-2016-4565
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-23 10:59:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The InfiniBand (aka IB) stack in the Linux kernel before 4.5.3 incorrectly relies on the write system call, which allows local u

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-264 | 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	So
[security-announce] SUSE-SU-2016:2001-1: important: Security update for	af
Red Hat Customer Portal	af
[security-announce] SUSE-SU-2016:1672-1: important: Security update for	af
USN-3021-2: Linux kernel (OMAP4) vulnerabilities | Ubuntu	af
[security-announce] SUSE-SU-2016:2010-1: important: Security update for	af
[security-announce] SUSE-SU-2016:2005-1: important: Security update for	af
kernel/git/torvalds/linux.git - Linux kernel source tree	af
[security-announce] SUSE-SU-2016:2007-1: important: Security update for	af
USN-3007-1: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	af
[security-announce] SUSE-SU-2016:2003-1: important: Security update for	af

Red Hat Customer Portal	af8
USN-3019-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu	af8
[security-announce] SUSE-SU-2016:1995-1: important: Security update for	af8
Red Hat Customer Portal	af8
Oracle VM Server for x86 Bulletin - July 2016	af8
USN-3021-1: Linux kernel vulnerabilities | Ubuntu	af8
[security-announce] SUSE-SU-2016:2014-1: important: Security update for	af8
USN-3002-1: Linux kernel (Wily HWE) vulnerabilities | Ubuntu	af8
[security-announce] SUSE-SU-2016:1937-1: important: Security update for	af8
USN-3005-1: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu	af8
Red Hat Customer Portal	af8
Red Hat Customer Portal	af8
[security-announce] SUSE-SU-2016:1690-1: important: Security update for	af8
Red Hat Customer Portal	af8
Oracle Linux Bulletin - July 2016	af8
Debian -- Security Information -- DSA-3607-1 linux	af8
[security-announce] openSUSE-SU-2016:2184-1: important: Security update	af8
Red Hat Customer Portal	af8
USN-3003-1: Linux kernel vulnerabilities | Ubuntu	af8
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.3	af8
Red Hat Customer Portal	af8
[security-announce] openSUSE-SU-2016:1641-1: important: Security update	af8
[security-announce] SUSE-SU-2016:2105-1: important: Security update for	af8
USN-3018-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	af8
USN-3004-1: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	af8
[security-announce] SUSE-SU-2016:1961-1: important: Security update for	af8
Red Hat Customer Portal	af8
[security-announce] SUSE-SU-2016:1994-1: important: Security update for	af8
USN-3001-1: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu	af8
Red Hat Customer Portal	af8
[security-announce] SUSE-SU-2016:2002-1: important: Security update for	af8
[security-announce] SUSE-SU-2016:2009-1: important: Security update for	af8
Oracle Linux Bulletin - April 2016	af8
oss-security - CVE Request: Linux: IB/security: Restrict use of the write() interface'	af8
1310570 – (CVE-2016-4565) CVE-2016-4565 kernel: infiniband: Unprivileged process can overwrite kernel memory using rdma_ucm.ko	af8

[security-announce] SUSE-SU-2016:1985-1: important: Security update for	af
USN-3006-1: Linux kernel vulnerabilities | Ubuntu	af
Linux Kernel CVE-2016-4565 Local Security Bypass Vulnerability	af
IB/security: Restrict use of the write() interface · torvalds/linux@e6bd18f · GitHub	af
[security-announce] SUSE-SU-2016:2011-1: important: Security update for	af
[security-announce] SUSE-SU-2016:2006-1: important: Security update for	af
USN-3018-1: Linux kernel vulnerabilities | Ubuntu	af
[security-announce] SUSE-SU-2016:2000-1: important: Security update for	af
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.