CVE-2016-3955

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

Summary

CVE	CVE-2016-3955
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-03 21:59:15 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The usbip_recv_xbuff function in drivers/usb/usbip/usbip_common.c in the Linux kernel before 4.5.3 allows remote attacker

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/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	Canonical	Ubuntu Linux	12.04	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	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
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
USN-3000-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu	af854a3a-2127-422b-91
USN-2998-1: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	af854a3a-2127-422b-91
1328478 – (CVE-2016-3955) CVE-2016-3955 Kernel: usbip: buffer overflow by trusting length of incoming packets	af854a3a-2127-422b-91
USN-2996-1: Linux kernel vulnerabilities | Ubuntu	af854a3a-2127-422b-91
Linux Kernel 'usbip/usbip_common.c' Remote Buffer Overflow Vulnerability	af854a3a-2127-422b-91

USN-3002-1: Linux kernel (Wily HWE) vulnerabilities | Ubuntu	af854a3a-2127-422b-91
Debian -- Security Information -- DSA-3607-1 linux	af854a3a-2127-422b-91
USN-2997-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	af854a3a-2127-422b-91
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-91
USN-2989-1: Linux kernel vulnerabilities | Ubuntu	af854a3a-2127-422b-91
USN-3003-1: Linux kernel vulnerabilities | Ubuntu	af854a3a-2127-422b-91
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.3	af854a3a-2127-422b-91
[security-announce] openSUSE-SU-2016:1641-1: important: Security update	af854a3a-2127-422b-91
USN-3004-1: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	af854a3a-2127-422b-91
USB: usbip: fix potential out-of-bounds write · torvalds/linux@b348d7d · GitHub	af854a3a-2127-422b-91
USN-3001-1: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu	af854a3a-2127-422b-91
oss-security - CVE Request: Linux kernel: remote buffer overflow in usbip	af854a3a-2127-422b-91
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.