CVE-2016-4951

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

Summary

CVE	CVE-2016-4951
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-23 10:59:15 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The tipc_nl_publ_dump function in net/tipc/socket.c in the Linux kernel through 4.6 does not verify socket existence, which a

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: NVD-CWE-Other | 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
oss-security - Re: CVE request: -- Linux kernel: Null pointer dereference in tipc_nl_publ_dump	af854a3a-2127-422b-91ae-364da2661108
Oracle VM Server for x86 Bulletin - October 2016	af854a3a-2127-422b-91ae-364da2661108
USN-3017-2: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108
USN-3016-3: Linux kernel (Qualcomm Snapdragon) vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108
USN-3016-4: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108
USN-3017-1: Linux kernel vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108
tipc: check nl sock before parsing nested attributes · torvalds/linux@45e093a · GitHub	af854a3a-2127-422b-91ae-364da2661108
Oracle Linux Bulletin - July 2016	af854a3a-2127-422b-91ae-364da2661108
USN-3020-1: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108
USN-3017-3: Linux kernel (Wily HWE) vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108

USN-3016-1: Linux kernel vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108
[security-announce] openSUSE-SU-2016:1641-1: important: Security update	af854a3a-2127-422b-91ae-364da2661108
netdev - BUG: net/tipc: NULL-ptr dereference in tipc_nl_publ_dump	af854a3a-2127-422b-91ae-364da2661108
USN-3016-2: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-91ae-364da2661108
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.