CVE-2016-9793

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

Summary

CVE	CVE-2016-9793
State	PUBLISHED
Assigner	mitre
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 sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative values of sk_sndbuf

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-119 | 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
kernel/git/torvalds/linux.git - Linux kernel source tree
Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remote Users
Red Hat Customer Portal
Red Hat Customer Portal
net: avoid signed overflows for SO_{SND|RCV}BUFFORCE · torvalds/linux@b98b0bc · GitHub
oss-security - Re: CVE Request: Linux: signed overflows for SO_{SND|RCV}BUFFORCE
Linux Kernel 'net/core/sock.c' Multiple Local Memory Corruption Vulnerabilities
kernel-exploits/CVE-2016-9793 at master · xairy/kernel-exploits · GitHub
Bug 1402013 – CVE-2016-9793 kernel: Signed overflow for SO_{SND|RCV}BUFFORCE
Android Security Bulletin—March 2017 | Android Open Source Project

Red Hat Customer Portal
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.8.14
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

378168 Virtuozzo Linux Security Update for perf (VZLSA-2017:0933)