CVE-2016-6828

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

Summary

CVE	CVE-2016-6828
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-16 21:59:08 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The tcp_check_send_head function in include/net/tcp.h in the Linux kernel before 4.7.5 does not properly maintain certain S

Risk And Classification

Primary CVSS: v3.0 5.5 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.000960000 probability, percentile 0.263170000 (date 2026-05-07)

Problem Types: CWE-416 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	4.9		AV:L/AC:L/Au:N/C:N/I:N/A:C

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:L/AC:L/Au:N/C:N/I:N/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
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.7.5	af854a3a-2127-422b-91ae-364da26611(
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-91ae-364da26611(
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da26611(
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da26611(
Bug 1367091 – CVE-2016-6828 kernel: Use after free in tcp_xmit_retransmit_queue	af854a3a-2127-422b-91ae-364da26611(
tcp: fix use after free in tcp_xmit_retransmit_queue() · torvalds/linux@bb1fcec · GitHub	af854a3a-2127-422b-91ae-364da26611(
[CVE-2016-6828] Linux kernel tcp related read Use After Free	af854a3a-2127-422b-91ae-364da26611(
Android Security Bulletin—November 2016 | Android Open Source Project	af854a3a-2127-422b-91ae-364da26611(
Linux Kernel 'tcp_xmit_retransmit_queue()' Function Use After Free Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da26611(

Linux Kernel tcp_xmit_retransmit_queue() Function Use After Free Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da26611
oss-security - Linux tcp_xmit_retransmit_queue use after free on 4.8-rc1 / master	af854a3a-2127-422b-91ae-364da26611
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da26611
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da26611
Red Hat Customer Portal	MITRE
Red Hat Customer Portal	MITRE
Red Hat Customer Portal	MITRE
Red Hat Customer Portal	MITRE
CVE-2016-6828 - Red Hat Customer Portal	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 378232 Virtuozzo Linux Security Update for kernel (VZLSA-2017:0036)
- 378250 Virtuozzo Linux Security Update for kernel-tools-libs (VZLSA-2017:0086)