CVE-2016-8655

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

Summary

CVE	CVE-2016-8655
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-08 08:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileges or cause 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: CWE-362 | CWE-416 | 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
[security-announce] SUSE-SU-2016:3117-1: important: Security update for
Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remote Users
Linux Kernel 4.4.0 AF_PACKET Race Condition / Privilege Escalation ≈ Packet Storm
Linux Kernel packet_set_ring() Race Condition Lets Local Users Obtain Root Privileges - SecurityTracker
Linux Kernel CVE-2016-8655 Local Race Condition Vulnerability
[security-announce] SUSE-SU-2016:3113-1: important: Security update for
USN-3151-1: Linux kernel vulnerability | Ubuntu
[security-announce] SUSE-SU-2016:3183-1: important: Security update for
[security-announce] SUSE-SU-2016:3205-1: important: Security update for
Red Hat Customer Portal

kernel/git/torvalds/linux.git - Linux kernel source tree
Bug 1400019 – CVE-2016-8655 kernel: Race condition in packet_set_ring leads to use after free
Linux 4.4.0 < 4.4.0-53 - 'AF_PACKET chocobo_root' Local Privilege Escalation (Metasploit) - Linux local Exploit
[security-announce] SUSE-SU-2016:3247-1: important: Security update for
oss-security - CVE-2016-8655 Linux af_packet.c race condition (local root)
[security-announce] SUSE-SU-2016:3169-1: important: Security update for
Red Hat Customer Portal
USN-3151-2: Linux kernel (Xenial HWE) vulnerability | Ubuntu
USN-3149-2: Linux kernel (Trusty HWE) vulnerability | Ubuntu
Red Hat Customer Portal
USN-3152-1: Linux kernel vulnerability | Ubuntu
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privilege Escalation
[security-announce] SUSE-SU-2016:3206-1: important: Security update for
USN-3150-2: Linux kernel (OMAP4) vulnerability | Ubuntu
USN-3149-1: Linux kernel vulnerability | Ubuntu
[security-announce] SUSE-SU-2016:3116-1: important: Security update for
Android Security Bulletin—March 2017 | Android Open Source Project
[security-announce] SUSE-SU-2016:3096-1: important: Security update for
USN-3152-2: Linux kernel (Raspberry Pi 2) vulnerability | Ubuntu
[security-announce] SUSE-SU-2016:3197-1: important: Security update for
USN-3151-4: Linux kernel (Raspberry Pi 2) vulnerability | Ubuntu
USN-3151-3: Linux kernel (Qualcomm Snapdragon) vulnerability | Ubuntu
packet: fix race condition in packet_set_ring · torvalds/linux@84ac726 · GitHub
USN-3150-1: Linux kernel vulnerability | Ubuntu
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
CVE-2016-8655 - Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

378284 Virtuozzo Linux Security Update for kernel-tools-libs (VZLSA-2017:0386)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**