CVE-2022-1247

Public on May 11, 2022
Last Modified: September 26, 2022 at 9:18:53 AM UTC

MODERATE

Moderate Impact
What does this mean?

7.8

CVSS v3 Base Score
CVSS Score Breakdown

Description

The MITRE CVE dictionary describes this issue as:

An issue found in linux-kernel that leads to a race condition in rose_connect(). The rose driver uses rose_neigh->use to represent how many objects are using the rose_neigh. When a user wants to delete a rose_route via rose_ioctl(), the rose driver calls rose_del_node() and removes neighbours only if their “count” and “use” are zero.

Statement

There was no shipped kernel version that was seen affected by this problem. These files are not built in our source code.

Additional Information

- Bugzilla 2066799: CVE-2022-1247 kernel: A race condition bug in rose_connect()
- CWE-362->CWE-366: Concurrent Execution using Shared Resource with Improper

Synchronization ('Race Condition') leads to Race Condition within a Thread

- FAQ: Frequently asked questions about CVE-2022-1247

Affected Packages and Issued Red Hat Security Errata

Platform	Package	State	Errata	Release Date
Red Hat Enterprise Linux 7	kernel-rt	Not affected		
Red Hat Enterprise Linux 8	kernel-rt	Not affected		
Red Hat Enterprise Linux 9	kernel-rt	Affected		
Red Hat Enterprise Linux 6	kernel	Not affected		
Red Hat Enterprise Linux 7	kernel	Not affected		
Red Hat Enterprise Linux 8	kernel	Not affected		
Red Hat Enterprise Linux 9	kernel	Affected		

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Common Vulnerability Scoring System (CVSS) Score Details

The following CVSS metrics and score provided are preliminary and subject to review.

CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	7.8	7.0
Attack Vector	Local	Local
Attack Complexity	Low	High
Privileges Required	Low	Low
User Interaction	None	None
Scope	Unchanged	Unchanged
Confidentiality	High	High
Integrity Impact	High	High
Availability Impact	High	High

CVSS v3 Vector

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

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

Acknowledgements

Red Hat would like to thank Beraphin for reporting this issue.

Frequently Asked Questions

Why is Red Hat's CVSS v3 score or Impact different from other vendors? ›

My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability? ›

What can I do if my product is listed as "Will not fix"? ›

Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected? ›

Not sure what something means? Check out our Security Glossary.

This page is generated automatically and has not been checked for errors or omissions. For clarification or corrections please contact Red Hat Product Security.

Last Modified: September 26, 2022 at 9:18:53 AM UTC