# Report on CVE-2024-43856

**Title: Vulnerability in Linux Kernel: CVE-2024-43856**

Submitted by: @generalzodx28

Submitted to: @.viper_11

Date: August 21, 2024

**1. Overview:**

CVE-2024-43856 is a vulnerability found in the Linux Kernel, particularly affecting the dmam_free_coherent function. This function frees a DMA allocation and then calls devres_destroy to remove the associated data structure. A race condition could occur where a concurrent task reuses the freed memory, leading to the possibility of multiple entries with the same address in the devres list, which can cause the wrong entry to be freed, triggering a system crash.

**2. Impact:**

This vulnerability can result in a critical system crash due to memory mismanagement, affecting systems reliant on the Linux kernel.

**3. Solution:**

The issue was resolved by modifying the call order to ensure that the devres entry is destroyed before freeing the DMA allocation, preventing the possibility of concurrent reuse.

**4. References:**

- [NVD Entry](https://nvd.nist.gov/vuln/detail/CVE-2024-43856)

- [Linux Kernel Git Commit](https://git.kernel.org/stable/c/257193083e8f43907e99ea633820fc2b3bcd24c7)

## 5. Conclusion:

This vulnerability highlights the importance of careful memory management in kernel operations, particularly in functions involving hardware communication like DMA. It is crucial for systems using affected kernel versions to apply the provided patches to avoid potential system instability.

*This report is created by Zeeshan Zafar for internal use.*