



# CVE-2021-3736

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2021-3736                                                                                                          |
| <b>State</b>           | PUBLIC                                                                                                                 |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                    |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                           |
| <b>Published</b>       | 2022-08-23 16:15:00 UTC                                                                                                |
| <b>Updated</b>         | 2022-08-25 02:28:00 UTC                                                                                                |
| <b>Description</b>     | A flaw was found in the Linux kernel. A memory leak problem was found in mbochs_ioctl in samples/vfio-mdev/mbochs.c in |

## Risk And Classification

**Problem Types:** CWE-401

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product      | Version | Update | Edition | Language |
|------------------|--------|--------------|---------|--------|---------|----------|
| Operating System | Linux  | Linux Kernel | All     | All    | All     | All      |

## References

| Reference                                                                                                     | Source  | Link                                |
|---------------------------------------------------------------------------------------------------------------|---------|-------------------------------------|
| Red Hat Customer Portal - Access to 24x7 support and knowledge                                                | MISC    | <a href="#">access.redhat.com</a>   |
| 1995570 – (CVE-2021-3736) CVE-2021-3736 kernel: uninitialized kernel stack may lead to information disclosure | MISC    | <a href="#">bugzilla.redhat.com</a> |
| vfio/mbochs: Fix missing error unwind of mbochs_used_mbytes · torvalds/linux@de5494a · GitHub                 | MISC    | <a href="#">github.com</a>          |
| CVE Program record                                                                                            | CVE.ORG | <a href="#">www.cve.org</a>         |
| NVD vulnerability detail                                                                                      | NVD     | <a href="#">nvd.nist.gov</a>        |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[184028](#) Debian Security Update for linux (CVE-2021-3736)

[902784](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10622)

[904000](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10622-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)