



# CVE-2022-1280

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

## Summary

<b>CVE</b>	CVE-2022-1280
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-13 18:15:00 UTC
<b>Updated</b>	2022-04-20 19:46:00 UTC
<b>Description</b>	A use-after-free vulnerability was found in drm_lease_held in drivers/gpu/drm/drm_lease.c in the Linux kernel due to a race

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

## References

### Reference

- oss-security - Linux kernel: A concurrency use-after-free between drm\_setmaster\_ioctl and drm\_mode\_getresources
- 2071022 – (CVE-2022-1280) CVE-2022-1280 kernel: concurrency use-after-free between drm\_setmaster\_ioctl and drm\_mode\_getresources
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- 160107 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9828)
- 160108 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9829)
- 160270 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-8267)

<a href="#">183842</a> Debian Security Update for linux (CVE-2022-1280)
<a href="#">240869</a> Red Hat Update for kernel-rt (RHSA-2022:7933)
<a href="#">240904</a> Red Hat Update for kernel security (RHSA-2022:8267)
<a href="#">671929</a> EulerOS Security Update for kernel (EulerOS-SA-2022-1999)
<a href="#">671975</a> EulerOS Security Update for kernel (EulerOS-SA-2022-2159)
<a href="#">672003</a> EulerOS Security Update for kernel (EulerOS-SA-2022-2134)
<a href="#">752120</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1651-1)
<a href="#">752125</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1686-1)
<a href="#">752126</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1687-1)
<a href="#">753176</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1676-1)
<a href="#">753252</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15 SP2) (SUSE-SU-2022:1849-1)
<a href="#">753299</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1669-1)
<a href="#">753330</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP4) (SUSE-SU-2022:2268-1)
<a href="#">753411</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 16 for SLE 15 SP3) (SUSE-SU-2022:1859-1)
<a href="#">753421</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 27 for SLE 12 SP5) (SUSE-SU-2022:1783-1)
<a href="#">753431</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 12 SP5) (SUSE-SU-2022:1796-1)
<a href="#">940798</a> AlmaLinux Security Update for kernel (ALSA-2022:8267)
<a href="#">940843</a> AlmaLinux Security Update for kernel-rt (ALSA-2022:7933)

© [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](#).

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