Unbreakable Enterprise Kernel

Unbreakable Enterprise Kernel Release 7 Update 1 - Release Notes (5.15.0-100)

F70414-09
March 2024

ORACLE

Unbreakable Enterprise Kernel Unbreakable Enterprise Kernel Release 7 Update 1 - Release Notes (5.15.0-100),

F70414-09

Contents

Preface

Unbreakable Enterprise Kernel Release 7 Update 1: Release Notes (5.15.0-100) provides a summary of the new features, significant changes, as well as any known issues in Unbreakable Enterprise Kernel Release 7 Update 1 (UEK R7U1).

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

Access to Oracle Support for Accessibility

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit https://www.oracle.com/corporate/accessibility/learning-support.html#support-tab.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

About Unbreakable Enterprise Kernel Release 7 Update 1

This chapter provides an overview of Unbreakable Enterprise Kernel Release 7 Update 1 (UEK R7U1) and contains important information about this major release.

> **Note:**
>
> Upgrading from an Unbreakable Enterprise Kernel Developer Preview release to its later official version isn't supported. If you're running the Developer Preview version, you must reinstall the official UEK release upon its general availability.

UEK R7U1 is initially released with the 5.15.0-100.96.32 version of the kernel. The kernel's source code is available through a public git source code repository at https://github.com/oracle/linux-uek.

The following is a general description of the scope of support for UEK R7U1:

- The kernel is developed, built, and tested on the 64-bit Arm (aarch64), Intel® 64-bit x86_64, and AMD 64-bit x86_64 architectures and is based on the mainline Linux kernel version 5.15.0.
- UEK R7U1 is made available for installation on the latest Oracle Linux 8 and Oracle Linux 9 update releases.
- In UEK R7U1, more features are enabled to provide support for key functional requirements and patches are applied to improve performance and optimize the kernel for use on Oracle operating environments. Note that Oracle actively monitors upstream check-ins and applies critical bug and security fixes to UEK R7U1.
- Although UEK R7U1 uses the same versioning model as the mainline Linux kernel version, it's possible that some applications might not understand the 5.15.0 versioning scheme. Note, however, that regular Linux applications are usually neither aware of nor affected by Linux kernel version numbers.

Certification of UEK R7 for Oracle Products

The following important information applies to the certification of Oracle products with UEK R7.

Note that certification of different Oracle products with UEK R7 might not be immediately available at the time of the UEK R7 release. Ensure that the product you're using is certified for use with UEK R7 before upgrading or installing the kernel. You can check for certification information at https://support.oracle.com/epmos/faces/CertifyHome.

Oracle Automatic Storage Management Cluster File System (Oracle ACFS) certification for different kernel versions is described in Document ID 1369107.1, which is available at https://support.oracle.com/epmos/faces/DocumentDisplay?id=1369107.1.

Oracle Automatic Storage Management Filter Driver (Oracle ASMFD) certification for different kernel versions is described in Document ID 2034681.1, which is available at https://support.oracle.com/epmos/faces/DocumentDisplay?id=2034681.1.

Compatibility

Oracle Linux maintains full user space compatibility with Red Hat Enterprise Linux (RHEL), which is independent of the kernel version that's running underneath the OS. Note that existing applications in user space continue to run unmodified with UEK R7; no recertifications are required for RHEL certified applications.

To minimize any impact on interoperability during releases, the Oracle Linux team works with third-party vendors that have hardware and software with dependencies on kernel modules. The kernel ABI for UEK R7 will remain unchanged in all subsequent updates to the initial release. Customers migrating from UEK6 must be aware that kernel ABIs have changed in UEK7. If an application is using kernel modules, users must verify the support status with the application vendor.

Notable changes in kernel headers

Upstream changes to kernel headers might mean that third-party modules do not compile across different kernel versions without modification to source code. Notably, the `memcg_cache_params` structure has been moved from `include/linux/slab.h` to `mm/slab.h`, which means that code needs to be refactored to account for the change if you are compiling across kernel versions.

To solve this problem so that the code can compile for UEK R6 and UEK R7, change the header requirements in the source code. For example, change lines like those in the following example to what is shown in the second example:

```
#ifdef CONFIG_SLUB
#include <linux/slub_def.h>
#endif
```

```
#if ( LINUX_VERSION_CODE < KERNEL_VERSION(5,4,0) )

#ifdef CONFIG_SLUB
#include <linux/slub_def.h>
#endif

#endif
```

2
New Features and Changes

This chapter describes new features, enhancements, and other notable changes that are introduced in UEK R7U1.

Optimized Memory for Containers

In this release, the `list_lru` internal kernel data structure is dynamically allocated. The previous static implementation allocated the data structure to memory `cgroup`s regardless of whether `cgroup`s use the data structure or not. With this update, the allocation of `list_lru` to `cgroup`s is delayed until needed, which ensures that memory is available for user applications especially on systems with a large number of running containers.

Intel® Advanced Matrix Extensions for Virtualization Enabled

Intel® Advanced Matrix Extensions (AMX) on 4th Gen Intel® Xeon® Scalable processors are enabled in the kernel. AMX is a new programming paradigm designed to accelerate artificial intelligence and machine learning workloads by providing a framework to work easily with matrices.

This update includes the kernel code required to enable AMX within virtualized environments running in QEMU 6.1 with the `-cpu host` option.

Perfmon V2 updates for AMD 4th Gen EPYC™ processors

Backports are included for AMD Performance Monitoring Version 2 (Perfmon V2) features on recent and upcoming AMD processors. Perfmon V2 allows you to set registers to enable or disable multiple performance counters at the same time and automatically detects the number of core Performance Monitor Counters (PMCs) rather than depending on a static settings per CPU family. The current updates also include the addition of L3 miss filtering, which works by tagging an instruction on Instruction Based Sampling (IBS) counter overflow and generating a Non Maskable Interrupt (NMI) if the tagged instruction causes an L3 miss. This feature is useful for feeding data to a page-migration daemon in tiered memory systems.

For more information about using `perf` to monitor system performance, see the `perf(1)` manual page.

NFSv4 Courteous Server Feature Enabled

This update release introduces the NFSv4 Courteous Server feature to help mitigate against the effects of network partitioning. NFSv4 is a stateful protocol that maintains leases for clients that track operations on the server. Network outages or partitions that cause a client's release renewal to fail can result in complex recovery processes that can fail. Even in scenarios where recovery processes do not fail, the state recovery process can take time to complete impacting performance and increasing load.

NFSv4 Courteous Server does not immediately expunge the client state on lease expiration and continues to recognize previously generated state tokens as valid until a conflict arises between the expired state and the requests from another client, or until the server reboots. This feature can avoid performing recovery where it may not be required.

A client that is set to `courtesy` status has the following characteristics:

- The client is expired but still has states on the server.
- The client does not own locks that are in waiter (conflict) state.
- The client has no conflict for any granted delegations.

The entire client lease is destroyed for a client in `courtesy` status under the following conditions:

- The client has conflicts with other client requests.
- The maximum number of NFS clients allowed on the system, based on system memory configuration, is reached.
- The available system memory drops to a level that triggers the memory shrinker process.

The `/proc/fs/nfsd/clients` interface is updated to reflect whether a client is in `courtesy` status. For example:

```
cat /proc/fs/nfsd/clients/2/info

clientid: 0xf0d156a662a0deec
address: "192.0.2.95:1003"
status: courtesy
seconds from last renew: 198
name: "Linux NFSv4.1 nfs.example.com"
minor version: 1
Implementation domain: "kernel.org"
Implementation name: "Linux 5.18.0-rc6+ #1 SMP PREEMPT_DYNAMIC Fri May 27
22:29:45 GMT 2022 x86_64"
Implementation time: [0, 0]
callback state: UP
callback address: 192.0.2.95:0
```

You can also use this interface to manually destroy a courtesy client. For example:

```
echo "expire" | sudo tee -a /proc/fs/nfsd/clients/2/ctl
```

Driver Updates

Unbreakable Enterprise Kernel Release 7 Update 1 supports a large number of hardware devices. In close cooperation with hardware and storage vendors, Oracle has updated several device drivers from the versions in mainline Linux 5.15.0.

The following new features are noted in the drivers that are shipped with UEK R7U1:

- **Broadcom BCM573xx network driver**

  The Broadcom BCM573xx network driver, `bnxt_en` is updated to include a large number of upstream and vendor supplied patches.

- **Broadcom Emulex Fibre Channel HBA driver**

The Broadcom Emulex LightPulse Fibre Channel SCSI driver, `lpfc`, is updated to version 14.2.0.5 with vendor supplied patches and bug fixes.

- **Microsoft Azure Network Adapter driver**

  The Microsoft Azure Network Adapter driver, `mana`, is included in this release. Upstream and vendor supplied patches are included and the driver is intended for use on Oracle Linux 8 and Oracle Linux 9. Notable feature updates include the addition of a handler for eXpress Data Path (XDP) Redirects.

- **MPI3 Storage Controller device driver**

  The MPI3 Storage Controller device driver, `mpi3mr`, is included in this release at version 8.2.0.3.0. Upstream and vendor supplied patches are included.

- **QLogic FastLinQ 4xxxx Core module**

  The QLogic FastLinQ 4xxxx Core module, `qed`, is updated to include vendor supplied patches to update this driver in line with upstream changes.

- **QLogic FastLinQ 4xxxx iSCSI module**

  The QLogic FastLinQ 4xxxx iSCSI module, `qedi`, is updated to include vendor supplied patches to update this driver in line with upstream changes. Notably, these ISCSI transport fixes include `iscsid` connection recovery fixes and `qedi` shutdown handler hang fixes.

- **Marvell QLogic Fibre Channel HBA driver**

  The Marvell QLogic Fibre Channel HBA driver, `qla2xxx`, is updated to version 10.02.08.100-k and includes a large number of vendor supplied patches and updates.

- **Intel® Ethernet Connection E800 Series Linux Driver**

  The Intel® Ethernet Connection E800 Series Linux Driver is updated to include vendor supplied patches and bug fixes.

CA Restrictions on Machine Keyring Removed

The `.machine` kernel keyring was introduced in UEK R7 and fully described in Unbreakable Enterprise Kernel Release 7: Release Notes (5.15.0-0.30). However, certification authority (CA) restrictions that were implemented did not accept Machine Owned Key (MOK) certificates without the CA bit set to be loaded into the `.machine` keyring.

With the removal of the restrictions, all MOK certificates can now be loaded.

For more information about secure booting, see Oracle Linux: Working With UEFI Secure Boot.

NVMe Verbose Logging

In this release, verbose logging for NVMe is enabled by default to improve logging. This implementation facilitates troubleshooting by helping administrators to better analyze why the controller might fail NVMe-related commands.

Secure Boot Enabled on All UEFI-Compliant Systems

Beginning with this update release, Secure Boot is implemented and kernel images are now signed on all UEFI-compliant x86_64 and Arm systems.

3
Known Issues

This chapter describes any known issues for Unbreakable Enterprise Kernel Release 7.

Unusable or Unavailable Features for the Arm Platform

The following are specific features that are known to not work, remain untested, or have issues that render the feature unusable.

- **InfiniBand**

  InfiniBand hardware is currently not supported for the Arm architecture when using UEK R7.

- **FibreChannel**

  FibreChannel hardware is currently not supported for the Arm architecture when using UEK R7.

- **RDMA**

  RDMA is not supported on the Arm platform.

dracut-install: ERROR: installing 'virtio' might be displayed during UEK R7 installation

In UEK R7, `virtio` isn't built as a module, but is built directly into the kernel. As such, you don't have to specify `virtio` in the dracut configuration file to add it to initramfs. If you previously had dracut configuration that included this module, attempting to install UEK R7 displays the following dracut error:

```
dracut-install: ERROR: installing 'virtio'
dracut: FAILED:  /usr/lib/dracut/dracut-install -D
/var/tmp/dracut.FOKWjy/initramfs --kerneldir
/lib/modules/5.15.0-0.21.1.el8uek.x86_64/ -m xen_netfront xen_blkfront
virtio_blk virtio_net virtio virtio_pci virtio_balloon hyperv_keyboard
hv_netvsc hid_hyperv hv_utils hv_storvsc hyperv_fb ahci libahci
dracut-install: ERROR: installing 'virtio'
dracut: FAILED:  /usr/lib/dracut/dracut-install -D
/var/tmp/dracut.G2XSGh/initramfs --kerneldir
/lib/modules/5.15.0-0.21.1.el8uek.x86_64/ -m xen_netfront xen_blkfront
virtio_blk virtio_net virtio virtio_pci virtio_balloon hyperv_keyboard
hv_netvsc hid_hyperv hv_utils hv_storvsc hyperv_fb ahci libahci
```

This error is displayed, regardless of whether you use the `yum` or `rpm` command to install UEK R7.

To work around the issue, before installing UEK R7, remove the "virtio" text from the dracut configuration file. Make sure to remove *only* the "virtio" text, leaving all other "virtio_*" entries intact, for example:

```
cat /etc/dracut.conf.d/01-dracut-vm.conf


add_drivers+=" xen_netfront xen_blkfront "
add_drivers+=" virtio_blk virtio_net virtio virtio_pci virtio_balloon "
add_drivers+=" hyperv_keyboard hv_netvsc hid_hyperv hv_utils hv_storvsc
hyperv_fb "
add_drivers+=" ahci libahci "
```

Use the following command to verify that `virtio` is built into the kernel:

```
grep CONFIG_VIRTIO= /boot/config-5.15.0-0.30.4.el8uek.x86_64
```

If `virtio` is built into the kernel, the output should be as follows:

```
CONFIG_VIRTIO=y
```

(Bug ID 33834972)

Upgrading from UEK R6 to UEK R7 on Arm platform may fail if RAID 5 default page size differs from default stripe size

Starting with UEK R7, the default page size on the Arm platform has changed to 4 KB, from the previous 64 KB default. This change in page size might cause an upgrade from UEK R6 to UEK R7 to fail on systems that are configured for RAID 5 when the default page size differs from the default stripe size.

For this reason, before upgrading from UEK R6 to UEK R7, back up and reformat RAID 5 volumes. In cases where retaining the same RAID 5 configuration is preferred, we recommend that you continue to run UEK R6.

See Default Page Size on Arm Platform Changed to 4 KB for additional information.

(Bug ID 33858264)

Swap partitions created on Arm platform using an earlier UEK release don't work after upgrade to UEK R7

The UEK R7 release includes a significant change for the Arm platform regarding the default page size, which has changed to 4 KB, from the previous 64 KB default. Any swap partitions that were created on the Arm platform using an earlier UEK release, for example, UEK R6, don't work after upgrading to UEK R7.

> **Note:**
>
> This issue applies to the Arm platform, irrespective of file system type.

Upon the first boot into UEK R7 after an upgrade, the following `systemd` service failure is indicated:

```
systemctl list-units --failed
UNIT LOAD ACTIVE SUB DESCRIPTION

dev-mapper-ol_myhost\x2dswap.swap loaded failed failed
/dev/mapper/ol_myhost-swap
```

To work around this issue, you must reinitialize the swap device with the new page size after upgrading to UEK R7. Use the `swapon` command as follows and specify the swap location:

```
sudo swapon --fixpgsz /dev/mapper/ol_myhost-swap


swapon: /dev/mapper/ol_myhost-swap: swap format pagesize does not match.
swapon: /dev/mapper/ol_myhost-swap: reinitializing the swap.
mkswap: /dev/mapper/ol_myhost-swap: warning: wiping old swap signature.
Setting up swapspace version 1, size = 2 GiB (2147479552 bytes)
no label, UUID=d7ef0a33-403f-447b-863f-d52b7f66c803
```

In the previous command, `/dev/mapper/ol_myhost-swap` is an example of a typical swap location that you might specify.

For more information about the important change in default page size for the Arm platform in UEK R7, see Default Page Size on Arm Platform Changed to 4 KB.

(Bug ID 34322552)

Cloud-init and systemd-udevd fail to rename mlx5_core network interfaces during upgrade from UEK R6 to UEK R7

During an upgrade from UEK R6 to UEK R7 on an Oracle Infrastructure instance, `cloud-init` and `systemd-udevd` revert to using the older UEK R6 device naming scheme (`ifcfg-ens300f0`) for the `mlx5_core` network interface, rather than correctly renaming the device with the new UEK R7 device naming scheme (`ens300f0np0`).

To ensure that the `mlx5_core` network interface does not revert to using the former UEK R6 device naming scheme, do the following after the upgrade to UEK R7 has completed, prior to rebooting the system:

1. Remove the old network configuration file, for example:

   ```
   sudo rm /etc/sysconfig/network-scripts/ifcfg-ens300f0
   ```

2. Remove any cached data saved by `cloud-init`:

   ```
   sudo cloud-init clean
   ```

3. Reboot the instance for the changes to take effect.

(Bug ID 34146775)

Mellanox NIC interface name subject to change after upgrading from UEK R6 to UEK R7

During a kernel upgrade from UEK R6 to UEK R7, the `mlx5_core` device name is subject to change, from `ens2f0` (UEK R6) to `ens2f0np0` (UEK R7).

You might encounter this issue under the following circumstances:

- When upgrading an Oracle Linux 8 system that is running UEK R6 to UEK R7.
- When upgrading an Oracle Linux 8 system that is running UEK R6 to Oracle Linux 9 (which ships with UEK R7 by default).
- When upgrading an Oracle Linux 8 system that is already running UEK R7 to Oracle Linux 9.

> **Note:**
>
> In the case where an Oracle Linux 8 system is already running UEK R7, if you previously configured the system to use backwards-compatible device names (`ens2f0`), you might need to apply the workaround that follows to your GRUB configuration after the upgrade to Oracle Linux 9 has completed.

Note that fresh installations of UEK R7 on Oracle Linux 8 and Oracle Linux 9 use the default naming convention for UEK R7 (`enp2s0f0np0`) by default.

To retain backwards-compatible (UEK R6) device names for the `mlx5_core` driver-based network interface card (NIC), perform the following workaround after upgrading to UEK R7, prior to rebooting your system. It is recommended that you back up your existing `grub.cfg` file before making this change.

1. Edit the `/etc/default/grub` file and append the end of the line in the `GRUB_CMDLINE_LINUX=` module as follows:

   ```
   GRUB_CMDLINE_LINUX="console=xxxx
   mlx5_core.expose_pf_phys_port_name=0"
   ```

2. After editing the file, locate the `grub.cfg` file on your system, then run the command to update GRUB configuration, as appropriate:

   - On BIOS-based systems, the `grub.cfg` output/target file is usually located at `/boot/grub2/grub.cfg` and you would run the following command:

     ```
     sudo grub2-mkconfig -o /boot/grub2/grub.cfg
     ```

- On UEFI-based systems, the `grub.cfg` output/target file could be located at `/etc/grub2-efi.cfg` or `/boot/efi/EFI/redhat/grub.cfg`. Depending on the location of the file, you would run one of the following commands:

  ```
  sudo grub2-mkconfig -o /etc/grub2-efi.cfg
  ```

  ```
  sudo grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
  ```

3. Reboot the system for the changes to take effect.

(Bug IDs 34103369, 34145887)

Random high CPU utilization issue encountered with database benchmark program

A random high CPU utilization issue has been encountered with the database benchmark program running on a 192-CPU virtual machine in Azure. This issue was initially discovered in Oracle Linux 8.4 and Ubuntu 20.04 (5.11.0-1022-azure); however, a complete fix for the issue isn't yet available in the upstream kernels.

This issue typically manifests itself with a >90% CPU utilization spike occurring every 1 to 2 minutes and lasting approximately 5 to 20 seconds, which degrades the system's performance significantly. When the CPU utilization spike is occurring, *each* of the 192 CPUs' %sys increases up to 60+%, and the %si increases up to 30%. In certain cases, the >90% CPU utilization spike has been observed 100% of the time.

To avoid encountering this issue, set the `dm_mod.dm_mq_queue_depth=256` kernel parameter.

(Bug ID 33665982)

(aarch64) Disk Encryption Password Prompt Not Being Displayed at System Boot

If you install Oracle Linux with GUI on an encrypted disk, for example, by choosing Server with GUI during the installation stage, and VGA is enabled, the password prompt doesn't appear on the VGA output at system boot. Consequently, the boot process can not be completed. The prompt appears only on a serial console, and therefore, you would need to switch to a serial console to provide the password there.

This issue is specific to systems on the Arm platform only and occurs regardless of whether you're using secure boot or not. Further, the issue applies to Oracle Linux 8 or Oracle Linux 9 systems that use UEKR6 or UEKR7.

To make the GUI password prompt for disk encryption appear at boot time on VGA output without using a serial console, add `plymouth.ignore-serial-consoles` to the kernel command line in the GRUB configuration. For instructions, see the *Managing Kernels and System Boot* chapter in Oracle Linux 9: Managing Core System Configuration.

(Bug ID 35034465)

(aarch64) Permission error message is displayed during firmware upgrade

When firmware is being updated on a system that's running UEKR7 with a version earlier than 5.15.0-104.119.4.2, an error similar to the following might be displayed. The error occurs typically on systems on the AMD platform.

```
/var/tmp/rpm-tmp.x8KEGx: line 9: /sys/devices/system/cpu/microcode/reload:
Permission denied
```

Code in the firmware package that triggers a reload is ignored because the kernel doesn't provide this facility. The message is harmless and can be ignored.

The reload facility is available in UEKR7 version 5.15.0-104.119.4.2 and later.

(Bug ID 35677123)

XFS DAX Mount Option Is Incompatible With Oracle Linux 9 With Reflink Enabled

On Oracle Linux 9 with UEK R7, the file system DAX mount option `dax=always` is incompatible with reflink-enabled XFS file systems. For example, running the command `sudo mount -o dax=always /dev/pmem1 /mnt` displays the following error:

```
mount: /mnt: wrong fs type, bad option, bad superblock on /dev/pmem1,
missing codepage
    or helper program, or other error.
mount: (hint) your fstab has been modified, but systemd still uses the
old version;
    use 'systemctl daemon-reload' to reload.
```

(Bug ID 35991195)

`xdp-tools` on Oracle Linux 9 Is Incompatible With UEK R7

The Oracle Linux 9 `xdp-tools` package that contains the `xdp-monitor` and `xdp-bench` commands is incompatible with UEK R7. The following errors are displayed when these commands are run on an Oracle Linux 9 system that's running UEK R7:

```
- END PROG LOAD LOG -
libbpf: prog 'tp_xdp_cpumap_kthread': failed to load: -22
libbpf: failed to load object 'xdp_sample'
libbpf: failed to load BPF skeleton 'xdp_sample': -22
```

If you need this package, use Oracle Linux 8 with `xdp-tools` v1.2.10-1.el8 or earlier.

(Bug ID 36014171)

4
List of CVEs fixed in this release

The following list describes the CVEs that are fixed in this release. The content provided here is automatically generated and includes the CVE identifier and a summary of the issue.

Note that CVEs are continually handled in patch updates that are made available as errata builds for the current release. For this reason, it is absolutely critical that you keep your system up to date with the latest package updates for this kernel release.

You can keep up to date with the latest CVE information at https://linux.oracle.com/cve.

- **CVE-2020-36516**

  An issue was discovered in the Linux kernel through 5.16.11. The mixed IPID assignment method with the hash-based IPID assignment policy allows an off-path attacker to inject data into a victim's TCP session or terminate that session.

  See https://linux.oracle.com/cve/CVE-2020-36516.html for more information.

- **CVE-2021-4083**

  A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigger a race condition. This flaw allows a local user to crash the system or escalate their privileges on the system. This flaw affects Linux kernel versions prior to 5.16-rc4.

  See https://linux.oracle.com/cve/CVE-2021-4083.html for more information.

- **CVE-2021-4135**

  A memory leak vulnerability was found in the Linux kernel's eBPF for the Simulated networking device driver in the way user uses BPF for the device such that function nsim_map_alloc_elem being called. A local user could use this flaw to get unauthorized access to some data.

- **CVE-2021-4155**

  A data leak flaw was found in the way XFS_IOC_ALLOCSP IOCTL in the XFS filesystem allowed for size increase of files with unaligned size. A local attacker could use this flaw to leak data on the XFS filesystem otherwise not accessible to them.

  See https://linux.oracle.com/cve/CVE-2021-4155.html for more information.

- **CVE-2021-4197**

  An unprivileged write to the file handler flaw in the Linux kernel's control groups and namespaces subsystem was found in the way users have access to some less privileged process that are controlled by cgroups and have higher privileged parent process. It is actually both for cgroup2 and cgroup1 versions of control groups. A local user could use this flaw to crash the system or escalate their privileges on the system.

  See https://linux.oracle.com/cve/CVE-2021-4197.html for more information.

- **CVE-2021-22600**

  A double free bug in packet_set_ring() in net/packet/af_packet.c can be exploited by a local user through crafted syscalls to escalate privileges or deny service. We recommend

upgrading kernel past the effected versions or rebuilding past ec6af094ea28f0f2dda1a6a33b14cd57e36a9755

See https://linux.oracle.com/cve/CVE-2021-22600.html for more information.

- **CVE-2021-33655**

  When sending malicous data to kernel by ioctl cmd FBIOPUT_VSCREENINFO,kernel will write memory out of bounds.

  See https://linux.oracle.com/cve/CVE-2021-33655.html for more information.

- **CVE-2021-39685**

  In various setup methods of the USB gadget subsystem, there is a possible out of bounds write due to an incorrect flag check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-210292376References: Upstream kernel

  See https://linux.oracle.com/cve/CVE-2021-39685.html for more information.

- **CVE-2021-43976**

  In the Linux kernel through 5.15.2, mwifiex_usb_recv in drivers/net/wireless/marvell/mwifiex/usb.c allows an attacker (who can connect a crafted USB device) to cause a denial of service (skb_over_panic).

  See https://linux.oracle.com/cve/CVE-2021-43976.html for more information.

- **CVE-2021-44733**

  A use-after-free exists in drivers/tee/tee_shm.c in the TEE subsystem in the Linux kernel through 5.15.11. This occurs because of a race condition in tee_shm_get_from_id during an attempt to free a shared memory object.

  See https://linux.oracle.com/cve/CVE-2021-44733.html for more information.

- **CVE-2021-45402**

  The check_alu_op() function in kernel/bpf/verifier.c in the Linux kernel through v5.16-rc5 did not properly update bounds while handling the mov32 instruction, which allows local users to obtain potentially sensitive address information, aka a "pointer leak."

- **CVE-2021-45480**

  An issue was discovered in the Linux kernel before 5.15.11. There is a memory leak in the __rds_conn_create() function in net/rds/connection.c in a certain combination of circumstances.

- **CVE-2022-0168**

  A denial of service (DOS) issue was found in the Linux kernel';s smb2_ioctl_query_info function in the fs/cifs/smb2ops.c Common Internet File System (CIFS) due to an incorrect return from the memdup_user function. This flaw allows a local, privileged (CAP_SYS_ADMIN) attacker to crash the system.

  See https://linux.oracle.com/cve/CVE-2022-0168.html for more information.

- **CVE-2022-0171**

  A flaw was found in the Linux kernel. The existing KVM SEV API has a vulnerability that allows a non-root (host) user-level application to crash the host kernel by creating a confidential guest VM instance in AMD CPU that supports Secure Encrypted Virtualization (SEV).

- **CVE-2022-0264**

  A vulnerability was found in the Linux kernel's eBPF verifier when handling internal data structures. Internal memory locations could be returned to userspace. A local attacker with the permissions to insert eBPF code to the kernel can use this to leak internal kernel memory details defeating some of the exploit mitigations in place for the kernel. This flaws affects kernel versions < v5.16-rc6

- **CVE-2022-0330**

  A random memory access flaw was found in the Linux kernel's GPU i915 kernel driver functionality in the way a user may run malicious code on the GPU. This flaw allows a local user to crash the system or escalate their privileges on the system.

  See https://linux.oracle.com/cve/CVE-2022-0330.html for more information.

- **CVE-2022-0382**

  An information leak flaw was found due to uninitialized memory in the Linux kernel's TIPC protocol subsystem, in the way a user sends a TIPC datagram to one or more destinations. This flaw allows a local user to read some kernel memory. This issue is limited to no more than 7 bytes, and the user cannot control what is read. This flaw affects the Linux kernel versions prior to 5.17-rc1.

- **CVE-2022-0492**

  A vulnerability was found in the Linux kernel';s cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.

  See https://linux.oracle.com/cve/CVE-2022-0492.html for more information.

- **CVE-2022-0494**

  A kernel information leak flaw was identified in the scsi_ioctl function in drivers/scsi/scsi_ioctl.c in the Linux kernel. This flaw allows a local attacker with a special user privilege (CAP_SYS_ADMIN or CAP_SYS_RAWIO) to create issues with confidentiality.

  See https://linux.oracle.com/cve/CVE-2022-0494.html for more information.

- **CVE-2022-0500**

  A flaw was found in unrestricted eBPF usage by the BPF_BTF_LOAD, leading to a possible out-of-bounds memory write in the Linux kernel';s BPF subsystem due to the way a user loads BTF. This flaw allows a local user to crash or escalate their privileges on the system.

- **CVE-2022-0617**

  A flaw null pointer dereference in the Linux kernel UDF file system functionality was found in the way user triggers udf_file_write_iter function for the malicious UDF image. A local user could use this flaw to crash the system. Actual from Linux kernel 4.2-rc1 till 5.17-rc2.

  See https://linux.oracle.com/cve/CVE-2022-0617.html for more information.

- **CVE-2022-0742**

  Memory leak in icmp6 implementation in Linux Kernel 5.13+ allows a remote attacker to DoS a host by making it go out-of-memory via icmp6 packets of type 130 or 131. We recommend upgrading past commit 2d3916f3189172d5c69d33065c3c21119fe539fc.

- **CVE-2022-0998**

An integer overflow flaw was found in the Linux kernel';s virtio device driver code in the way a user triggers the vhost_vdpa_config_validate function. This flaw allows a local user to crash or potentially escalate their privileges on the system.

- **CVE-2022-1011**

  A use-after-free flaw was found in the Linux kernel';s FUSE filesystem in the way a user triggers write(). This flaw allows a local user to gain unauthorized access to data from the FUSE filesystem, resulting in privilege escalation.

  See https://linux.oracle.com/cve/CVE-2022-1011.html for more information.

- **CVE-2022-1012**

  A memory leak problem was found in the TCP source port generation algorithm in net/ipv4/tcp.c due to the small table perturb size. This flaw may allow an attacker to information leak and may cause a denial of service problem.

  See https://linux.oracle.com/cve/CVE-2022-1012.html for more information.

- **CVE-2022-1055**

  A use-after-free exists in the Linux Kernel in tc_new_tfilter that could allow a local attacker to gain privilege escalation. The exploit requires unprivileged user namespaces. We recommend upgrading past commit 04c2a47ffb13c29778e2a14e414ad4cb5a5db4b5

  See https://linux.oracle.com/cve/CVE-2022-1055.html for more information.

- **CVE-2022-1184**

  A use-after-free flaw was found in fs/ext4/namei.c:dx_insert_block() in the Linux kernel';s filesystem sub-component. This flaw allows a local attacker with a user privilege to cause a denial of service.

  See https://linux.oracle.com/cve/CVE-2022-1184.html for more information.

- **CVE-2022-1462**

  An out-of-bounds read flaw was found in the Linux kernel';s TeleTYpe subsystem. The issue occurs in how a user triggers a race condition using ioctls TIOCSPTLCK and TIOCGPTPEER and TIOCSTI and TCXONC with leakage of memory in the flush_to_ldisc function. This flaw allows a local user to crash the system or read unauthorized random data from memory.

- **CVE-2022-1652**

  Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a concurrency use-after-free flaw in the bad_flp_intr function. By executing a specially-crafted program, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

  See https://linux.oracle.com/cve/CVE-2022-1652.html for more information.

- **CVE-2022-1789**

  With shadow paging enabled, the INVPCID instruction results in a call to kvm_mmu_invpcid_gva. If INVPCID is executed with CR0.PG=0, the invlpg callback is not set and the result is a NULL pointer dereference.

- **CVE-2022-1882**

  A use-after-free flaw was found in the Linux kernel';s pipes functionality in how a user performs manipulations with the pipe post_one_notification() after free_pipe_info() that is already called. This flaw allows a local user to crash or potentially escalate their privileges on the system.

- **CVE-2022-1943**

  A flaw out of bounds memory write in the Linux kernel UDF file system functionality was found in the way user triggers some file operation which triggers udf_write_fi(). A local user could use this flaw to crash the system or potentially

- **CVE-2022-1972**

  An out-of-bound write vulnerability was identified within the netfilter subsystem which can be exploited to achieve privilege escalation to root.

- **CVE-2022-1998**

  A use after free in the Linux kernel File System notify functionality was found in the way user triggers copy_info_records_to_user() call to fail in copy_event_to_user(). A local user could use this flaw to crash the system or potentially escalate their privileges on the system.

  See https://linux.oracle.com/cve/CVE-2022-1998.html for more information.

- **CVE-2022-2078**

  A vulnerability was found in the Linux kernel's nft_set_desc_concat_parse() function .This flaw allows an attacker to trigger a buffer overflow via nft_set_desc_concat_parse() , causing a denial of service and possibly to run code.

  See https://linux.oracle.com/cve/CVE-2022-2078.html for more information.

- **CVE-2022-2153**

  A flaw was found in the Linux kernel';s KVM when attempting to set a SynIC IRQ. This issue makes it possible for a misbehaving VMM to write to SYNIC/STIMER MSRs, causing a NULL pointer dereference. This flaw allows an unprivileged local attacker on the host to issue specific ioctl calls, causing a kernel oops condition that results in a denial of service.

  See https://linux.oracle.com/cve/CVE-2022-2153.html for more information.

- **CVE-2022-2196**

  A regression exists in the Linux Kernel within KVM: nVMX that allowed for speculative execution attacks. L2 can carry out Spectre v2 attacks on L1 due to L1 thinking it doesn't need retpolines or IBPB after running L2 due to KVM (L0) advertising eIBRS support to L1. An attacker at L2 with code execution can execute code on an indirect branch on the host machine. We recommend upgrading to Kernel 6.2 or past commit 2e7eab81425a

- **CVE-2022-2503**

  Dm-verity is used for extending root-of-trust to root filesystems. LoadPin builds on this property to restrict module/firmware loads to just the trusted root filesystem. Device-mapper table reloads currently allow users with root privileges to switch out the target with an equivalent dm-linear target and bypass verification till reboot. This allows root to bypass LoadPin and can be used to load untrusted and unverified kernel modules and firmware, which implies arbitrary kernel execution and persistence for peripherals that do not verify firmware updates. We recommend upgrading past commit 4caae58406f8ceb741603eee460d79bacca9b1b5

  See https://linux.oracle.com/cve/CVE-2022-2503.html for more information.

- **CVE-2022-2585**

  A use-after-free flaw was found in the Linux kernel';s POSIX CPU timers functionality in the way a user creates and then deletes the timer in the non-leader thread of the program. This flaw allows a local user to crash or potentially escalate their privileges on the system.

See https://linux.oracle.com/cve/CVE-2022-2585.html for more information.

- **CVE-2022-2586**

  A use-after-free flaw was found in nf_tables cross-table in the net/netfilter/nf_tables_api.c function in the Linux kernel. This flaw allows a local, privileged attacker to cause a use-after-free problem at the time of table deletion, possibly leading to local privilege escalation.

  See https://linux.oracle.com/cve/CVE-2022-2586.html for more information.

- **CVE-2022-2588**

  A use-after-free flaw was found in route4_change in the net/sched/cls_route.c filter implementation in the Linux kernel. This flaw allows a local, privileged attacker to crash the system, possibly leading to a local privilege escalation issue.

  See https://linux.oracle.com/cve/CVE-2022-2588.html for more information.

- **CVE-2022-2602**

  A race issue between handling an io_uring request and the Unix socket garbage collector was found in the Linux kernel. This flaw allows an attacker to have local privilege escalation.

  See https://linux.oracle.com/cve/CVE-2022-2602.html for more information.

- **CVE-2022-2639**

  An integer coercion error was found in the openvswitch kernel module. Given a sufficiently large number of actions, while copying and reserving memory for a new action of a new flow, the reserve_sfa_size() function does not return -EMSGSIZE as expected, potentially leading to an out-of-bounds write access. This flaw allows a local user to crash or potentially escalate their privileges on the system.

  See https://linux.oracle.com/cve/CVE-2022-2639.html for more information.

- **CVE-2022-2663**

  An issue was found in the Linux kernel in nf_conntrack_irc where the message handling can be confused and incorrectly matches the message. A firewall may be able to be bypassed when users are using unencrypted IRC with nf_conntrack_irc configured.

  See https://linux.oracle.com/cve/CVE-2022-2663.html for more information.

- **CVE-2022-2873**

  An out-of-bounds memory access flaw was found in the Linux kernel Intel';s iSMT SMBus host controller driver in the way a user triggers the I2C_SMBUS_BLOCK_DATA (with the ioctl I2C_SMBUS) with malicious input data. This flaw allows a local user to crash the system.

  See https://linux.oracle.com/cve/CVE-2022-2873.html for more information.

- **CVE-2022-2905**

  An out-of-bounds memory read flaw was found in the Linux kernel's BPF subsystem in how a user calls the bpf_tail_call function with a key larger than the max_entries of the map. This flaw allows a local user to gain unauthorized access to data.

- **CVE-2022-2938**

A flaw was found in the Linux kernel's implementation of Pressure Stall Information. While the feature is disabled by default, it could allow an attacker to crash the system or have other memory-corruption side effects.

See https://linux.oracle.com/cve/CVE-2022-2938.html for more information.

- **CVE-2022-2959**

  A race condition was found in the Linux kernel's watch queue due to a missing lock in pipe_resize_ring(). The specific flaw exists within the handling of pipe buffers. The issue results from the lack of proper locking when performing operations on an object. This flaw allows a local user to crash the system or escalate their privileges on the system.

  See https://linux.oracle.com/cve/CVE-2022-2959.html for more information.

- **CVE-2022-2964**

  A flaw was found in the Linux kernel';s driver for the ASIX AX88179_178A-based USB 2.0/3.0 Gigabit Ethernet Devices. The vulnerability contains multiple out-of-bounds reads and possible out-of-bounds writes.

  See https://linux.oracle.com/cve/CVE-2022-2964.html for more information.

- **CVE-2022-2977**

  A flaw was found in the Linux kernel implementation of proxied virtualized TPM devices. On a system where virtualized TPM devices are configured (this is not the default) a local attacker can create a use-after-free and create a situation where it may be possible to escalate privileges on the system.

- **CVE-2022-3028**

  A race condition was found in the Linux kernel's IP framework for transforming packets (XFRM subsystem) when multiple calls to xfrm_probe_algs occurred simultaneously. This flaw could allow a local attacker to potentially trigger an out-of-bounds write or leak kernel heap memory by performing an out-of-bounds read and copying it into a socket.

  See https://linux.oracle.com/cve/CVE-2022-3028.html for more information.

- **CVE-2022-3077**

  A buffer overflow vulnerability was found in the Linux kernel Intel';s iSMT SMBus host controller driver in the way it handled the I2C_SMBUS_BLOCK_PROC_CALL case (via the ioctl I2C_SMBUS) with malicious input data. This flaw could allow a local user to crash the system.

  See https://linux.oracle.com/cve/CVE-2022-3077.html for more information.

- **CVE-2022-3104**

  An issue was discovered in the Linux kernel through 5.16-rc6. lkdtm_ARRAY_BOUNDS in drivers/misc/lkdtm/bugs.c lacks check of the return value of kmalloc() and will cause the null pointer dereference.

- **CVE-2022-3105**

  An issue was discovered in the Linux kernel through 5.16-rc6. uapi_finalize in drivers/infiniband/core/uverbs_uapi.c lacks check of kmalloc_array().

- **CVE-2022-3106**

  An issue was discovered in the Linux kernel through 5.16-rc6. ef100_update_stats in drivers/net/ethernet/sfc/ef100_nic.c lacks check of the return value of kmalloc().

- **CVE-2022-3107**

An issue was discovered in the Linux kernel through 5.16-rc6. netvsc_get_ethtool_stats in drivers/net/hyperv/netvsc_drv.c lacks check of the return value of kvmalloc_array() and will cause the null pointer dereference.

- **CVE-2022-3108**

  An issue was discovered in the Linux kernel through 5.16-rc6. kfd_parse_subtype_iolink in drivers/gpu/drm/amd/amdkfd/kfd_crat.c lacks check of the return value of kmemdup().

- **CVE-2022-3115**

  An issue was discovered in the Linux kernel through 5.16-rc6. malidp_crtc_reset in drivers/gpu/drm/arm/malidp_crtc.c lacks check of the return value of kzalloc() and will cause the null pointer dereference.

- **CVE-2022-3169**

  A flaw was found in the Linux kernel. A denial of service flaw may occur if there is a consecutive request of the NVME_IOCTL_RESET and the NVME_IOCTL_SUBSYS_RESET through the device file of the driver, resulting in a PCIe link disconnect.

- **CVE-2022-3239**

  A flaw use after free in the Linux kernel video4linux driver was found in the way user triggers em28xx_usb_probe() for the Empia 28xx based TV cards. A local user could use this flaw to crash the system or potentially escalate their privileges on the system.

  See https://linux.oracle.com/cve/CVE-2022-3239.html for more information.

- **CVE-2022-3303**

  A race condition flaw was found in the Linux kernel sound subsystem due to improper locking. It could lead to a NULL pointer dereference while handling the SNDCTL_DSP_SYNC ioctl. A privileged local user (root or member of the audio group) could use this flaw to crash the system, resulting in a denial of service condition

  See https://linux.oracle.com/cve/CVE-2022-3303.html for more information.

- **CVE-2022-3435**

  A vulnerability classified as problematic has been found in Linux Kernel. This affects the function fib_nh_match of the file net/ipv4/fib_semantics.c of the component IPv4 Handler. The manipulation leads to out-of-bounds read. It is possible to initiate the attack remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-210357 was assigned to this vulnerability.

- **CVE-2022-3526**

  A vulnerability classified as problematic was found in Linux Kernel. This vulnerability affects the function macvlan_handle_frame of the file drivers/net/macvlan.c of the component skb. The manipulation leads to memory leak. The attack can be initiated remotely. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211024.

- **CVE-2022-3542**

  A vulnerability classified as problematic was found in Linux Kernel. This vulnerability affects the function bnx2x_tpa_stop of the file drivers/net/ethernet/broadcom/bnx2x/bnx2x_cmn.c of the component BPF. The manipulation leads to

memory leak. It is recommended to apply a patch to fix this issue. VDB-211042 is the identifier assigned to this vulnerability.

- **CVE-2022-3545**

  A vulnerability has been found in Linux Kernel and classified as critical. Affected by this vulnerability is the function area_cache_get of the file drivers/net/ethernet/netronome/nfp/nfpcore/nfp_cppcore.c of the component IPsec. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier VDB-211045 was assigned to this vulnerability.

  See https://linux.oracle.com/cve/CVE-2022-3545.html for more information.

- **CVE-2022-3565**

  A vulnerability, which was classified as critical, has been found in Linux Kernel. Affected by this issue is the function del_timer of the file drivers/isdn/mISDN/l1oip_core.c of the component Bluetooth. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211088.

  See https://linux.oracle.com/cve/CVE-2022-3565.html for more information.

- **CVE-2022-3577**

  An out-of-bounds memory write flaw was found in the Linux kernel';s Kid-friendly Wired Controller driver. This flaw allows a local user to crash or potentially escalate their privileges on the system. It is in bigben_probe of drivers/hid/hid-bigbenff.c. The reason is incorrect assumption - bigben devices all have inputs. However, malicious devices can break this assumption, leaking to out-of-bound write.

- **CVE-2022-3586**

  A flaw was found in the Linux kernel';s networking code. A use-after-free was found in the way the sch_sfb enqueue function used the socket buffer (SKB) cb field after the same SKB had been enqueued (and freed) into a child qdisc. This flaw allows a local, unprivileged user to crash the system, causing a denial of service.

  See https://linux.oracle.com/cve/CVE-2022-3586.html for more information.

- **CVE-2022-3594**

  A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function intr_callback of the file drivers/net/usb/r8152.c of the component BPF. The manipulation leads to logging of excessive data. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211363.

  See https://linux.oracle.com/cve/CVE-2022-3594.html for more information.

- **CVE-2022-3619**

  A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function l2cap_recv_acldata of the file net/bluetooth/l2cap_core.c of the component Bluetooth. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. VDB-211918 is the identifier assigned to this vulnerability.

- **CVE-2022-3623**

  A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function follow_page_pte of the file mm/gup.c of the component BPF. The manipulation leads to race condition. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211921 was assigned to this vulnerability.

- **CVE-2022-3625**

  A vulnerability was found in Linux Kernel. It has been classified as critical. This affects the function devlink_param_set/devlink_param_get of the file net/core/devlink.c of the component IPsec. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier VDB-211929 was assigned to this vulnerability.

- **CVE-2022-3628**

  A buffer overflow flaw was found in the Linux kernel Broadcom Full MAC Wi-Fi driver. This issue occurs when a user connects to a malicious USB device. This can allow a local user to crash the system or escalate their privileges.

  See https://linux.oracle.com/cve/CVE-2022-3628.html for more information.

- **CVE-2022-3629**

  A vulnerability was found in Linux Kernel. It has been declared as problematic. This vulnerability affects the function vsock_connect of the file net/vmw_vsock/af_vsock.c. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. VDB-211930 is the identifier assigned to this vulnerability.

  See https://linux.oracle.com/cve/CVE-2022-3629.html for more information.

- **CVE-2022-3640**

  A vulnerability, which was classified as critical, was found in Linux Kernel. Affected is the function l2cap_conn_del of the file net/bluetooth/l2cap_core.c of the component Bluetooth. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211944.

  See https://linux.oracle.com/cve/CVE-2022-3640.html for more information.

- **CVE-2022-3903**

  An incorrect read request flaw was found in the Infrared Transceiver USB driver in the Linux kernel. This issue occurs when a user attaches a malicious USB device. A local user could use this flaw to starve the resources, causing denial of service or potentially crashing the system.

- **CVE-2022-4129**

  A flaw was found in the Linux kernel's Layer 2 Tunneling Protocol (L2TP). A missing lock when clearing sk_user_data can lead to a race condition and NULL pointer dereference. A local user could use this flaw to potentially crash the system causing a denial of service.

  See https://linux.oracle.com/cve/CVE-2022-4129.html for more information.

- **CVE-2022-4139**

  An incorrect TLB flush issue was found in the Linux kernel';s GPU i915 kernel driver, potentially leading to random memory corruption or data leaks. This flaw could allow a local user to crash the system or escalate their privileges on the system.

  See https://linux.oracle.com/cve/CVE-2022-4139.html for more information.

- **CVE-2022-4378**

  A stack overflow flaw was found in the Linux kernel's SYSCTL subsystem in how a user changes certain kernel parameters and variables. This flaw allows a local user to crash or potentially escalate their privileges on the system.

  See https://linux.oracle.com/cve/CVE-2022-4378.html for more information.

- **CVE-2022-4662**

  A flaw incorrect access control in the Linux kernel USB core subsystem was found in the way user attaches usb device. A local user could use this flaw to crash the system.

  See https://linux.oracle.com/cve/CVE-2022-4662.html for more information.

- **CVE-2022-20368**

  Product: AndroidVersions: Android kernelAndroid ID: A-224546354References: Upstream kernel

  See https://linux.oracle.com/cve/CVE-2022-20368.html for more information.

- **CVE-2022-21385**

  A flaw in net_rds_alloc_sgs() in Oracle Linux kernels allows unprivileged local users to crash the machine. CVSS 3.1 Base Score 6.2 (Availability impacts). CVSS Vector (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

  See https://linux.oracle.com/cve/CVE-2022-21385.html for more information.

- **CVE-2022-21505**

  Linux kernel lockdown bypass using IMA.

  See https://linux.oracle.com/cve/CVE-2022-21505.html for more information.

- **CVE-2022-21546**

  *** UNKNOWN ***

  See https://linux.oracle.com/cve/CVE-2022-21546.html for more information.

- **CVE-2022-22942**

  A use-after-free flaw was found in the Linux kernel';s vmw_execbuf_copy_fence_user function in drivers/gpu/drm/vmwgfx/vmwgfx_execbuf.c in vmwgfx. This flaw allows a local attacker with user privileges to cause a privilege escalation problem.

  See https://linux.oracle.com/cve/CVE-2022-22942.html for more information.

- **CVE-2022-23222**

  kernel/bpf/verifier.c in the Linux kernel through 5.15.14 allows local users to gain privileges because of the availability of pointer arithmetic via certain *_OR_NULL pointer types.

- **CVE-2022-23816**

  RetBleed Arbitrary Speculative Code Execution with Return Instructions

  See https://linux.oracle.com/cve/CVE-2022-23816.html for more information.

- **CVE-2022-24122**

  kernel/ucount.c in the Linux kernel 5.14 through 5.16.4, when unprivileged user namespaces are enabled, allows a use-after-free and privilege escalation because a ucounts object can outlive its namespace.

- **CVE-2022-24448**

  An issue was discovered in fs/nfs/dir.c in the Linux kernel before 5.16.5. If an application sets the O_DIRECTORY flag, and tries to open a regular file, nfs_atomic_open() performs a regular lookup. If a regular file is found, ENOTDIR should occur, but the server instead returns uninitialized data in the file descriptor.

  See https://linux.oracle.com/cve/CVE-2022-24448.html for more information.

- **CVE-2022-25636**

  net/netfilter/nf_dup_netdev.c in the Linux kernel 5.4 through 5.6.10 allows local users to gain privileges because of a heap out-of-bounds write. This is related to nf_tables_offload.

  See https://linux.oracle.com/cve/CVE-2022-25636.html for more information.

- **CVE-2022-26966**

  An issue was discovered in the Linux kernel before 5.16.12. drivers/net/usb/sr9700.c allows attackers to obtain sensitive information from heap memory via crafted frame lengths from a device.

  See https://linux.oracle.com/cve/CVE-2022-26966.html for more information.

- **CVE-2022-27666**

  A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw allows a local attacker with a normal user privilege to overwrite kernel heap objects and may cause a local privilege escalation threat.

  See https://linux.oracle.com/cve/CVE-2022-27666.html for more information.

- **CVE-2022-27950**

  In drivers/hid/hid-elo.c in the Linux kernel before 5.16.11, a memory leak exists for a certain hid_parse error condition.

  See https://linux.oracle.com/cve/CVE-2022-27950.html for more information.

- **CVE-2022-28893**

  The SUNRPC subsystem in the Linux kernel through 5.17.2 can call xs_xprt_free before ensuring that sockets are in the intended state.

  See https://linux.oracle.com/cve/CVE-2022-28893.html for more information.

- **CVE-2022-29156**

  drivers/infiniband/ulp/rtrs/rtrs-clt.c in the Linux kernel before 5.16.12 has a double free related to rtrs_clt_dev_release.

- **CVE-2022-29581**

  Improper Update of Reference Count vulnerability in net/sched of Linux Kernel allows local attacker to cause privilege escalation to root. This issue affects: Linux Kernel versions prior to 5.18; version 4.14 and later versions.

  See https://linux.oracle.com/cve/CVE-2022-29581.html for more information.

- **CVE-2022-29901**

  Intel® microprocessor generations 6 to 8 are affected by a new Spectre variant that is able to bypass their retpoline mitigation in the kernel to leak arbitrary data. An attacker with unprivileged user access can hijack return instructions to achieve arbitrary speculative code execution under certain microarchitecture-dependent conditions.

  See https://linux.oracle.com/cve/CVE-2022-29901.html for more information.

- **CVE-2022-30594**

  The Linux kernel before 5.17.2 mishandles seccomp permissions. The PTRACE_SEIZE code path allows attackers to bypass intended restrictions on setting the PT_SUSPEND_SECCOMP flag.

See https://linux.oracle.com/cve/CVE-2022-30594.html for more information.

- **CVE-2022-32250**

  net/netfilter/nf_tables_api.c in the Linux kernel through 5.18.1 allows a local user (able to create user/net namespaces) to escalate privileges to root because an incorrect NFT_STATEFUL_EXPR check leads to a use-after-free.

  See https://linux.oracle.com/cve/CVE-2022-32250.html for more information.

- **CVE-2022-32296**

  The Linux kernel before 5.17.9 allows TCP servers to identify clients by observing what source ports are used. This occurs because of use of Algorithm 4 ("Double-Hash Port Selection Algorithm") of RFC 6056.

- **CVE-2022-33981**

  drivers/block/floppy.c in the Linux kernel before 5.17.6 is vulnerable to a denial of service, because of a concurrency use-after-free flaw after deallocating raw_cmd in the raw_cmd_ioctl function.

  See https://linux.oracle.com/cve/CVE-2022-33981.html for more information.

- **CVE-2022-34494**

  rpmsg_virtio_add_ctrl_dev in drivers/rpmsg/virtio_rpmsg_bus.c in the Linux kernel before 5.18.4 has a double free.

- **CVE-2022-34495**

  rpmsg_probe in drivers/rpmsg/virtio_rpmsg_bus.c in the Linux kernel before 5.18.4 has a double free.

- **CVE-2022-34918**

  An issue was discovered in the Linux kernel through 5.18.9. A type confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a local attacker to escalate privileges, a different vulnerability than CVE-2022-32250. (The attacker can obtain root access, but must start with an unprivileged user namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data in net/netfilter/nf_tables_api.c.

  See https://linux.oracle.com/cve/CVE-2022-34918.html for more information.

- **CVE-2022-36879**

  An issue was discovered in the Linux kernel through 5.18.14. xfrm_expand_policies in net/xfrm/xfrm_policy.c can cause a refcount to be dropped twice.

  See https://linux.oracle.com/cve/CVE-2022-36879.html for more information.

- **CVE-2022-36946**

  nfqnl_mangle in net/netfilter/nfnetlink_queue.c in the Linux kernel through 5.18.14 allows remote attackers to cause a denial of service (panic) because, in the case of an nf_queue verdict with a one-byte nfta_payload attribute, an skb_pull can encounter a negative skb->len.

  See https://linux.oracle.com/cve/CVE-2022-36946.html for more information.

- **CVE-2022-39188**

  An issue was discovered in include/asm-generic/tlb.h in the Linux kernel before 5.19. Because of a race condition (unmap_mapping_range versus munmap), a device driver can free a page while it still has stale TLB entries. This only occurs in situations with VM_PFNMAP VMAs.

- **CVE-2022-39189**

  An issue was discovered the x86 KVM subsystem in the Linux kernel before 5.18.17. Unprivileged guest users can compromise the guest kernel because TLB flush operations are mishandled in certain KVM_VCPU_PREEMPTED situations.

- **CVE-2022-39190**

  An issue was discovered in net/netfilter/nf_tables_api.c in the Linux kernel before 5.19.6. A denial of service can occur upon binding to an already bound chain.

  See https://linux.oracle.com/cve/CVE-2022-39190.html for more information.

- **CVE-2022-40307**

  An issue was discovered in the Linux kernel through 5.19.8. drivers/firmware/efi/capsule-loader.c has a race condition with a resultant use-after-free.

- **CVE-2022-40476**

  A null pointer dereference issue was discovered in fs/io_uring.c in the Linux kernel before 5.15.62. A local user could use this flaw to crash the system or potentially cause a denial of service.

- **CVE-2022-40768**

  drivers/scsi/stex.c in the Linux kernel through 5.19.9 allows local users to obtain sensitive information from kernel memory because stex_queuecommand_lck lacks a memset for the PASSTHRU_CMD case.

  See https://linux.oracle.com/cve/CVE-2022-40768.html for more information.

- **CVE-2022-41218**

  In drivers/media/dvb-core/dmxdev.c in the Linux kernel through 5.19.10, there is a use-after-free caused by refcount races, affecting dvb_demux_open and dvb_dmxdev_release.

  See https://linux.oracle.com/cve/CVE-2022-41218.html for more information.

- **CVE-2022-41850**

  roccat_report_event in drivers/hid/hid-roccat.c in the Linux kernel through 5.19.12 has a race condition and resultant use-after-free in certain situations where a report is received while copying a report->value is in progress.

  See https://linux.oracle.com/cve/CVE-2022-41850.html for more information.

- **CVE-2022-41858**

  A flaw was found in the Linux kernel. A NULL pointer dereference may occur while a slip driver is in progress to detach in sl_tx_timeout in drivers/net/slip/slip.c. This issue could allow an attacker to crash the system or leak internal kernel information.

  See https://linux.oracle.com/cve/CVE-2022-41858.html for more information.

- **CVE-2022-42703**

  mm/rmap.c in the Linux kernel before 5.19.7 has a use-after-free related to leaf anon_vma double reuse.

  See https://linux.oracle.com/cve/CVE-2022-42703.html for more information.

- **CVE-2022-42895**

  There is an infoleak vulnerability in the Linux kernel's net/bluetooth/l2cap_core.c's l2cap_parse_conf_req function which can be used to leak kernel pointers

remotely. We recommend upgrading past commit https://github.com/torvalds/linux/commit/b1a2cd50c0357f243b7435a732b4e62ba3157a2e https://www.google.com/url

See https://linux.oracle.com/cve/CVE-2022-42895.html for more information.

- **CVE-2022-42896**

  There are use-after-free vulnerabilities in the Linux kernel's net/bluetooth/l2cap_core.c's l2cap_connect and l2cap_le_connect_req functions which may allow code execution and leaking kernel memory (respectively) remotely via Bluetooth. A remote attacker could execute code leaking kernel memory via Bluetooth if within proximity of the victim. We recommend upgrading past commit https://www.google.com/url https://github.com/torvalds/linux/commit/711f8c3fb3db61897080468586b970c87c61d9e4 https://www.google.com/url

  See https://linux.oracle.com/cve/CVE-2022-42896.html for more information.

- **CVE-2022-43750**

  drivers/usb/mon/mon_bin.c in usbmon in the Linux kernel before 5.19.15 and 6.x before 6.0.1 allows a user-space client to corrupt the monitor's internal memory.

  See https://linux.oracle.com/cve/CVE-2022-43750.html for more information.

- **CVE-2022-43945**

  The Linux kernel NFSD implementation prior to versions 5.19.17 and 6.0.2 are vulnerable to buffer overflow. NFSD tracks the number of pages held by each NFSD thread by combining the receive and send buffers of a remote procedure call (RPC) into a single array of pages. A client can force the send buffer to shrink by sending an RPC message over TCP with garbage data added at the end of the message. The RPC message with garbage data is still correctly formed according to the specification and is passed forward to handlers. Vulnerable code in NFSD is not expecting the oversized request and writes beyond the allocated buffer space. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

  See https://linux.oracle.com/cve/CVE-2022-43945.html for more information.

- **CVE-2022-45869**

  A race condition in the x86 KVM subsystem in the Linux kernel through 6.1-rc6 allows guest OS users to cause a denial of service (host OS crash or host OS memory corruption) when nested virtualisation and the TDP MMU are enabled.

  See https://linux.oracle.com/cve/CVE-2022-45869.html for more information.

- **CVE-2022-45884**

  An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvbdev.c has a use-after-free, related to dvb_register_device dynamically allocating fops.

  See https://linux.oracle.com/cve/CVE-2022-45884.html for more information.

- **CVE-2022-45885**

  An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_frontend.c has a race condition that can cause a use-after-free when a device is disconnected.

  See https://linux.oracle.com/cve/CVE-2022-45885.html for more information.

- **CVE-2022-45886**

  An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_net.c has a .disconnect versus dvb_device_open race condition that leads to a use-after-free.

See https://linux.oracle.com/cve/CVE-2022-45886.html for more information.

- **CVE-2022-45887**

  An issue was discovered in the Linux kernel through 6.0.9. drivers/media/usb/ttusb-dec/ttusb_dec.c has a memory leak because of the lack of a dvb_frontend_detach call.

  See https://linux.oracle.com/cve/CVE-2022-45887.html for more information.

- **CVE-2022-45919**

  An issue was discovered in the Linux kernel through 6.0.10. In drivers/media/dvb-core/dvb_ca_en50221.c, a use-after-free can occur is there is a disconnect after an open, because of the lack of a wait_event.

  See https://linux.oracle.com/cve/CVE-2022-45919.html for more information.

- **CVE-2022-45934**

  An issue was discovered in the Linux kernel through 6.0.10. l2cap_config_req in net/bluetooth/l2cap_core.c has an integer wraparound via L2CAP_CONF_REQ packets.

  See https://linux.oracle.com/cve/CVE-2022-45934.html for more information.

- **CVE-2022-47929**

  In the Linux kernel before 6.1.6, a NULL pointer dereference bug in the traffic control subsystem allows an unprivileged user to trigger a denial of service (system crash) via a crafted traffic control configuration that is set up with "tc qdisc" and "tc class" commands. This affects qdisc_graft in net/sched/sch_api.c.

  See https://linux.oracle.com/cve/CVE-2022-47929.html for more information.

- **CVE-2023-0179**

  A buffer overflow vulnerability was found in the Netfilter subsystem in the Linux Kernel. This issue could allow the leakage of both stack and heap addresses, and potentially allow Local Privilege Escalation to the root user via arbitrary code execution.

  See https://linux.oracle.com/cve/CVE-2023-0179.html for more information.

- **CVE-2023-0266**

  A use after free vulnerability exists in the ALSA PCM package in the Linux Kernel. SNDRV_CTL_IOCTL_ELEM_{READ|WRITE}32 is missing locks that can be used in a use-after-free that can result in a priviledge escalation to gain ring0 access from the system user. We recommend upgrading past commit 56b88b50565cd8b946a2d00b0c83927b7ebb055e

  See https://linux.oracle.com/cve/CVE-2023-0266.html for more information.

- **CVE-2023-0394**

  A NULL pointer dereference flaw was found in rawv6_push_pending_frames in net/ipv6/raw.c in the network subcomponent in the Linux kernel. This flaw causes the system to crash.

  See https://linux.oracle.com/cve/CVE-2023-0394.html for more information.

- **CVE-2023-0468**

  A use-after-free flaw was found in io_uring/poll.c in io_poll_check_events in the io_uring subcomponent in the Linux Kernel due to a race condition of poll_refs. This flaw may cause a NULL pointer dereference.

- **CVE-2023-23454**

  cbq_classify in net/sched/sch_cbq.c in the Linux kernel through 6.1.4 allows attackers to cause a denial of service (slab-out-of-bounds read) because of type confusion (non-negative numbers can sometimes indicate a TC_ACT_SHOT condition rather than valid classification results).

  See https://linux.oracle.com/cve/CVE-2023-23454.html for more information.

- **CVE-2023-23455**

  atm_tc_enqueue in net/sched/sch_atm.c in the Linux kernel through 6.1.4 allows attackers to cause a denial of service because of type confusion (non-negative numbers can sometimes indicate a TC_ACT_SHOT condition rather than valid classification results).

  See https://linux.oracle.com/cve/CVE-2023-23455.html for more information.

- **CVE-2023-23559**

  In rndis_query_oid in drivers/net/wireless/rndis_wlan.c in the Linux kernel through 6.1.5, there is an integer overflow in an addition.

  See https://linux.oracle.com/cve/CVE-2023-23559.html for more information.

5
Installation and Availability

This chapter provides information about the availability of UEK R7 on Oracle Linux and includes installation and instructions on upgrading from a previous UEK release to UEK R7.

UEK R7 is supported on the Intel® 64-bit x86_64, AMD 64-bit x86_64 and 64-bit Arm (aarch64) platforms.

About Upgrading From a Previous Oracle Linux or UEK Release to UEK R7

UEK R7 is made available for installation on Oracle Linux 8, starting with the Oracle Linux 8.5 release. By default, Oracle Linux 9 ships with UEK R7.

The suggested migration path for upgrading the system from an earlier UEK release to UEK R7 is as follows:

- If you're running Oracle Linux 7 with an earlier UEK release, upgrade the operating system to the latest Oracle Linux 8 release. For instructions on upgrading the Oracle Linux 7 system, see Oracle Linux 8: Upgrading Systems With Leapp.
- If you're running an Oracle Linux 8 release that's earlier than Oracle Linux 8.5 with UEK R6, first upgrade the system to the latest Oracle Linux 8 update release. From here, you can upgrade to UEK R7. If you're already running Oracle Linux 8.5 or later with UEK R6, you can directly upgrade the system to UEK R7.

  For instructions on upgrading an Oracle Linux 8 system to Oracle Linux 9, see Oracle Linux 9: Upgrading Systems With Leapp.

Important:

In UEK R7, the default page size for the 64-bit Arm (aarch64) architecture has changed to 4 KB default, from the previous 64 KB default. The new 4 KB default page size might have significant implications on Arm-based systems that are running Oracle Linux 8 with an earlier UEK release, with either a Btrfs or an XFS file system.

- If an Arm-based system uses a Btrfs or an XFS file system, and you're running Oracle Linux 8 with an earlier UEK release, you might not be able to upgrade to UEK R7 without first migrating data to an alternative file system. The default on-disk file system block size is set to be the equivalent of the page size for these file systems, which means that the change in page size can render the file system inaccessible and can cause data corruption.

  Note, however, that Oracle has placed checks within the UEK R7 Arm RPM that prevent the installation of UEK R7 if a Btrfs file system is detected and the resulting change in block size could cause data to become inaccessible.
- For an XFS file system, the default block size is 4 KB. XFS enables you to manually set the block size at file system creation time. If you have XFS file systems with a block size greater than 4 KB, you are required to migrate data before upgrading to UEK R7.

  Typically, a data migration plan might involve adding another storage device, formatting it with an unaffected file system or using XFS with the block size specified as 4 KB, and then moving your data onto the newly formatted device.
- Users of the Oracle Linux 8 developer image installed on Raspberry Pi systems are necessarily affected because the image uses a Btrfs file system, by default. If you're using this image, and you intend to upgrade to UEK R7, you must migrate data to an alternative unaffected file system before trying to install UEK R7. For more information about using the Raspberry Pi hardware platform, see Install Oracle Linux on a Raspberry Pi.
- Any existing swap partitions that were created on the Arm platform using an earlier UEK release, such as UEK R6, don't work after upgrading to UEK R7. The change to a 4 KB default page size on the aarch64 platform requires that any existing swap partitions on the system *must* be reinitialized with the new page size after booting the system with UEK R7. For further details, see Swap partitions created on Arm platform using an earlier UEK release don't work after upgrade to UEK R7.

For general information about working with file systems in Oracle Linux 8, see Oracle Linux 8: Managing Local File Systems.

Obtaining Packages for Installation

If you have a subscription to Oracle Unbreakable Linux support, you can obtain the packages for UEK R7 by registering your system with the Unbreakable Linux Network (ULN) and then subscribing it to additional channels. See Subscribing to ULN Channels.

If your system is not registered with ULN, you can obtain most of the required packages from the Oracle Linux yum server. See Enabling Access to Oracle Linux Yum Server Repositories.

When you have subscribed your system to the appropriate ULN channels or to the Oracle Linux yum server, you can proceed to upgrade your system to UEK R7. See Upgrading a System to UEK R7.

Enabling Access to Oracle Linux Yum Server Repositories

Packages for UEK R7 and any associated user space applications are available on the Oracle Linux yum server at https://yum.oracle.com/.

For Oracle Linux 8, the kernel images and all the associated user space packages for both the x86_64 and aarch64 platforms are made available by enabling the following repositories:

- `ol8_UEKR7`
- `ol8_baseos_latest`

For Oracle Linux 9, the kernel images and all the associated user space packages for both the x86_64 and aarch64 platforms are made available by enabling the following repositories:

- `ol9_UEKR7`
- `ol9_baseos_latest`

To enable access to repositories on the Oracle Linux yum server, use the `dnf config-manager` command and specify the appropriate repositories for the release that you're running.

For example, you would enable access to the Oracle Linux 8 repositories as follows:

```
sudo dnf config-manager --enable ol8_baseos_latest ol8_UEKR7
```

> **Note:**
>
> You can only use the `dnf config-manager` to enable or disable repositories that already have a configuration file for the specified repository. Repository configurations are typically stored in the `/etc/yum.repos.d` file. The repository configurations that are required to install the UEK release on Oracle Linux 8 and Oracle Linux 9 are included in the `oraclelinux-release-el8` and `oraclelinux-release-el9` packages, respectively. Note that you might need to update the package to the latest version to obtain the correct yum repository configuration.

Subscribing to ULN Channels

For Oracle Linux 8, kernel image and user space packages are made available for the x86_64 platform in the following ULN channels:

- `ol8_x86_64_UEKR7`
- `ol8_x86_64_baseos_latest`

For Oracle Linux 8, kernel image and user space packages are made available for the aarch64 platform in the following ULN channels:

- `ol8_aarch64_UEKR7`
- `ol8_aarch64_baseos_latest`

For Oracle Linux 9, kernel image and user space packages are made available for the x86_64 platform in the following ULN channels:

- `ol9_x86_64_UEKR7`
- `ol9_x86_64_baseos_latest`

For Oracle Linux 9, kernel image and user space packages are made available for the aarch64 platform in the following ULN channels:

- `ol9_aarch64_UEKR7`
- `ol9_aarch64_baseos_latest`

The following instructions assume that you have previously registered your system with ULN.

To subscribe a system to a ULN channel:

1. Sign in to https://linux.oracle.com with a ULN username and password.
2. On the Systems tab, in the list of registered machines, click the link that corresponds to the name of the system.
3. On the System Details page, click **Manage Subscriptions**.
4. On the System Summary page, from the list of available channels, select each of the required channels, then click the right arrow to move the selected channel to the list of subscribed channels.
5. Click **Save Subscriptions**.

For more information about using ULN, see Oracle Linux: Managing Software on Oracle Linux.

Upgrading a System to UEK R7

The following instructions describe how to upgrade a system to UEK R7. For more details about the suggested migration paths for upgrading to UEK R7, see About Upgrading From a Previous Oracle Linux or UEK Release to UEK R7.

1. Enable access to the appropriate ULN channels or yum repositories, as described in Subscribing to ULN Channels and Enabling Access to Oracle Linux Yum Server Repositories.

   > **Tip:**
   >
   > Disable any other UEK channels or repositories that you might have previously configured as good practice.

2. After enabling access to the appropriate channels or repositories, upgrade the system to UEK R7 by running the following commands:

   ```
   sudo dnf install -y kernel-uek
   sudo dnf update -y
   ```

3. After the upgrade has completed, reboot the system.

   Ensure to select the UEK R7 kernel (version 5.15.0) if it's not the default boot kernel.

For questions regarding installing software or updating a system, see Oracle Linux: Managing Software on Oracle Linux.

Installing and Upgrading Oracle-Supported RDMA Packages on Oracle Linux

The following instructions describe how to install and upgrade Oracle-supported RDMA packages on Oracle Linux 8 and Oracle Linux 9.

Installing Oracle-Supported RDMA Packages on Oracle Linux 8

> **Note:**
>
> These instructions apply to the x86_64 platform.

The following instructions describe how to install RDMA release packages (`oracle-rdma-release`) on an Oracle Linux 8 system. These instructions include steps on how to remove other previously installed RDMA packages that could cause conflicts when installing the `oracle-rdma-release` packages.

If you running Oracle Linux 9, see Installing Oracle-Supported RDMA Packages on Oracle Linux 9 for instructions.

1. Subscribe your system to the appropriate RDMA ULN channel or yum repository.

   - If you are using the Oracle Linux yum server, enable the `ol8_UEKR7_RDMA` repository for Oracle Linux 8, for example:

     ```
     sudo dnf config-manager --enable ol8_baseos_latest ol8_UEKR7
     ol8_UEKR7_RDMA
     ```

   - If you are using ULN, subscribe to `ol8_x86_64_UEKR7_RDMA` channel.

   For additional instructions, see Subscribing to ULN Channels and Enabling Access to Oracle Linux Yum Server Repositories.

2. Remove any existing packages that are related to RDMA, for example:

   ```
   sudo dnf remove 'ibacm*'
   sudo dnf remove 'ibutils*'
   sudo dnf remove 'infiniband-diags*'
   sudo dnf remove 'libibacl*'
   sudo dnf remove 'libibcm*'
   sudo dnf remove 'libibmad*'
   sudo dnf remove 'libibumad*'
   sudo dnf remove 'libibverbs*'
   sudo dnf remove 'librdmacm*'
   sudo dnf remove 'mstflint*'
   ```

```
sudo dnf remove 'opensm*'
sudo dnf remove 'oracle-rdma-tools'
sudo dnf remove 'perftest*'
sudo dnf remove 'qperf*'
sudo dnf remove 'rdma*'
sudo dnf remove 'rds-tools*'
sudo dnf remove 'rdma-core*'
```

3. Clean the yum cached files from all of the enabled repositories:

```
sudo dnf clean all
```

4. Install the RDMA packages for UEK R7.
   - If you are installing the packages on a bare-metal system, use the following command:

     ```
     sudo dnf install oracle-rdma-release
     ```

   - If you are installing the packages on a virtual platform (either a Xen hypervisor or a KVM guest), use the following command:

     ```
     sudo dnf install oracle-rdma-release-guest
     ```

   - (Optional) If you require the `libpcap` package, you must install this package separately:

     ```
     sudo dnf install libpcap
     ```

Each UEK release requires a different set of RDMA packages. If you change the kernel on your system to a UEK release that is earlier than UEK R7, use the following command to remove the existing UEK-based RDMA packages before installing the correct packages for the new kernel:

```
sudo dnf remove --setopt=clean_requirements_on_remove=1 oracle-rdma-
release
```

Note that the previous command might not work for all of the related packages. For example, in Oracle Linux 8, the `libpcap` package is a dependency for key system packages and therefore cannot be removed. Instead, you can use the `dnf history undo` command as follows to roll back and remove the dependencies for the `rdma-core` package:

```
sudo dnf history undo rdma-core
```

> **Caution:**
>
> Downgrading UEK versions is not advised, except for testing purposes.

Installing Oracle-Supported RDMA Packages on Oracle Linux 9

> **Note:**
>
> These instructions apply to the x86_64 platform.

The process of installing Oracle-supported RDMA packages on Oracle Linux 9 has been simplified through the use of new, user space packages, as well as a dedicated ULN channel and yum repository for RDMA-related packages.

If you are running Oracle Linux 8, the process of installing Oracle-supported RDMA packages remains the same as it was in previous releases. For instructions, see Installing Oracle-Supported RDMA Packages on Oracle Linux 8.

The following instructions describe how to install RDMA release packages (`oracle-rdma-release`) on an Oracle Linux 9 system:

1. Ensure that you have subscribed to the ULN channel or have enabled the yum repository that contains the RDMA-related user space packages for Oracle Linux 9.
   - If you are installing packages from ULN, subscribe to the `ol9_x86_64_RDMA` channel.
   - If you are installing packages from the Oracle Linux yum server, enable the `ol9_RDMA` yum repository.
2. Clean the yum cached files from all of the enabled repositories by running the following command:

   ```
   sudo dnf clean all
   ```

3. Install the RDMA packages for UEK R7:
   - If you are installing the packages on a bare-metal system, run the following command:

     ```
     sudo dnf install oracle-rdma-release
     ```

   - If you are installing the packages on a virtualized platform (either on a Xen hypervisor or KVM guest), run the following command:

     ```
     sudo dnf install oracle-rdma-release-guest
     ```

4. (Optional) If you require the `libpcap` package, you must install this package separately:

   ```
   sudo dnf install libpcap
   ```

Upgrading Oracle-Supported RDMA Packages on Oracle Linux 8 and Oracle Linux 9

You can upgrade the Oracle-supported RDMA packages on Oracle Linux 8 and Oracle Linux 9 by using the `dnf update` command.

If you are upgrading a system that has the `oracle-rdma-release` or `oracle-rdma-release-guest` package installed, if the package version is lower than version 0.18.1-1 and you intend to upgrade to version 0.18.1-1, or later, you must first manually remove the `rdma-core-devel` package. You should remove this package by using the `rpm -e --nodeps` command, which removes the package outside of the standard yum or DNF package manager control and leaves any dependencies intact, for example:

```
sudo /bin/rpm -e --nodeps rdma-core-devel
sudo dnf update
```