Unbreakable Enterprise Kernel

Unbreakable Enterprise Kernel Release 7 Update 2 - Release Notes (Version 5.15.0-200)

F82626-04
November 2023

Unbreakable Enterprise Kernel Unbreakable Enterprise Kernel Release 7 Update 2 - Release Notes (Version 5.15.0-200),

F82626-04

Contents

Preface

1 About Unbreakable Enterprise Kernel Release 7 Update 2

2 New Features and Changes

3 Known Issues

Preface

Unbreakable Enterprise Kernel Release 7 Update 2: Release Notes (5.15.0-200) provides a summary of the new features, significant changes, and any known issues in Unbreakable Enterprise Kernel Release 7 Update 2 (UEK R7U2).

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/.

For information about the accessibility of the Oracle Help Center, see the Oracle Accessibility Conformance Report at https://www.oracle.com/corporate/accessibility/templates/t2-11535.html.

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 2

This chapter provides an overview of Unbreakable Enterprise Kernel Release 7 Update 2 (UEK R7U2) 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 R7U2 is initially released with the 5.15.0-200.131.27 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 R7U2:

- 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 R7U2 is made available for installation on the latest Oracle Linux 8 and Oracle Linux 9 update releases.
- In UEK R7U2, 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 R7U2.
- Although UEK R7U2 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 R7U2.

NVMe In-Band Authentication for Data Protection

NVMe In-Band authentication is a security feature for NVMe over Fabrics configurations. NVMe In-Band authentication provides a challenge-response identify authentication protocol that uses a "shared secret" and doesn't require the transmission of a password between the host and controller. Authentication doesn't require a secure channel to remain safe. In this feature implementation, functionality is added to both the host and target side and driven by the user space `nvme-cli` application. The `nvme-cli` application must be at version 2.2.3 or later to use this feature.

NVMe In-Band authentication is available on Oracle Linux 9 with UEK R7U2.

AMD Last Branch Record Extension Version 2

The Last Branch Record (LBR) feature is a hardware based mechanism that's used to analyze the flow of control in software. It logs branch information in real time to enable the system to determine where priority or hot code should be directed, such as different types of optimizations that are active in running applications. This UEK release implements AMD Last Branch Record Extension Version 2 (LbrExtV2), whose added functionalities include LBR-Freeze-on-PMI to correlate better with PMC overflow events, new speculation information, and new hardware based filtering for obtaining data on specific branch types.

Kernel SYN Flood Messages Include the Listening Address

Kernel SYN flood messages are enhanced to include both the listening IP address and port:

```
Possible SYN flooding on port <ip_address>:<port>.
```

The update makes it easier for administrators to identify the affected socket when many processes are bound to the same port on different IP addresses.

Updated Drivers

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 R7U2:

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

  The Intel Ethernet Connection E800 Series Linux driver `ice` is updated to 6.0.0 with vendor supplied enhancements and bug fixes. Notable enhancements include Point-to-

Point Protocol over Ethernet (`PPPoE`) protocol hardware offload, Inter-Integrated Circuit (`I2C`) protocol write command, VLAN Tag Protocol Identifier (`TPID`) filters in the Ethernet switch device driver model (`switchdev`), and double VLAN tagging in `switchdev`. The update also includes changes to enable the driver to work with the Ethernet Port Configuration Tool (EPCT) that includes the `devlink` command, used to list and view configurable devices.

- **Mellanox 5th generation network adapters (ConnectX series) core driver**

  The Mellanox ConnectX series driver `mlx5` is updated to version 6.3 with vendor supplied patches and bug fixes.

- **Broadcom Emulex Fibre Channel HBA driver**

  The Broadcom Emulex Fibre Channel HBA driver `lpfc` is updated to version 14.2.0.13 with vendor supplied patches and bug fixes.

- **Marvell QLogic Fibre Channel HBA driver**

  The Marvell QLogic Fibre Channel HBA driver `qla2xxx` is updated to version 10.02.09.100-k with vendor supplied patches and bug fixes.

- **LSI MPT Fusion SAS 3.0 Device Driver**

  The LSI MPT Fusion SAS 3.0 Device Driver `mpt3sas` is updated to version 43.100.00.00 with vendor supplied patches and bug fixes.

- **Broadcom MegaRAID SAS driver**

  The Broadcom MegaRAID SAS driver `megaraid_sas` is updated to version 07.725.01.00-rc1 with vendor supplied patches and bug fixes.

- **MPI3 Storage Controller Device Driver**

  The MPI3 Storage Controller Device Driver `mpi3mr` is updated to version 8.5.0.0 with vendor supplied patches and bug fixes.

- **Broadcom BCM573xx network driver**

  The Broadcom BCM573xx network driver `bnxt_en` is updated with vendor supplied patches and is at version 6.2.

- **Microsoft Azure Network Adapter**

  The Microsoft Azure Network Adapter `mana` is updated with vendor supplied patches and bug fixes and is at version 6.4.

- **Solarflare network driver**

  The Solarflare network driver (`sfc`) has been split into `sfc` and `sfc-siena`. The latter (`sfc-siena`) is the driver for Siena hardware (SFN5000/SFN6000 series).

Deprecated and Removed Features

The following features are deprecated or removed and no longer available in UEK R7U2:

- **`CONFIG_RPCSEC_GSS_KRB5_ENCTYPES_DES` option for 3DES/DES3 RPCSEC GSS encryption types**

  The RPCSEC GSS encryption types DES and Triple-DES (3DES/DES3) are deprecated in this UEK release, and might be removed from the kernel in a future UEK release.

These encryption types were deprecated by RFCs 6649 and 8429 because they're known to be insecure.

- **`CONFIG_NFS_V2` and `CONFIG_NFSD_V2` options for NFSv2 client and server**
  Support for NFSv2 clients and NFSv2 servers is deprecated in this UEK release, and might be removed from the kernel in a future UEK release.

  NFSv2 has long been replaced by NFSv3 and NFSv4, which offer improved functionality, performance, and security.

- **`CONFIG_NFS_DISABLE_UDP_SUPPORT` option for NFSv3 over UDP**
  Support for NFS version 3 over the UDP network protocol is deprecated in this UEK release, and might be removed from the kernel in a future UEK release.

  Modern NFS/RPC over TCP and RDMA implementations provide better performance than UDP, and provide reliable ordered delivery of data combined with congestion control.

  Note that NFSv4 is already not supported over UDP, for the same reasons.

- **`CONFIG_STAGING` option**

  With the `CONFIG_STAGING` kernel configuration option, you can select drivers that don't necessarily meet the highest kernel quality level but are merely made available for test use. However, the kernel option `CONFIG_STAGING` is deprecated in this UEK release and might be removed in a future release.

- **`CONFIG_IXGB` option**
  The `CONFIG_IXGB` for Intel PRO/10GbE hardware is deprecated and might be removed from the kernel in a future UEK release.

- **`CONFIG_IP_NF_TARGET_CLUSTERIP` option**
  The `CONFIG_IP_NF_TARGET_CLUSTERIP` option that allowed you to build load-balancing clusters of network servers without a dedicated load-balancing router or switch is deprecated in favor of functionality already in Netfilter cluster match.

- **`CONFIG_EFI_VARS` option**
  The `CONFIG_EFI_VARS` option that provided the `efivars` sysfs interface to configure UEFI variables is removed from the upstream kernel and is deprecated in this release of UEK. Replacement functionality has been present in the kernel since 2012. For more information, see https://www.kernel.org/doc/html/latest/filesystems/efivarfs.html.

- **Firewire driver**

  The `CONFIG_FIREWIRE` option was disabled in Oracle Linux 9. Thus, the Firewire driver is deprecated and unusable in this UEK release.

- **`crashkernel=auto` option**

  The `crashkernel=auto` option is deprecated and no longer supported on Oracle Linux 9 and therefore unsupported for UEK R7 on Oracle Linux 9. Some platforms, such as the Raspberry Pi have maximum limits for `crashkernel` memory reservation and these must be specified explicitly. This option will be removed in a future UEK release.

- **Several network scheduler modules**

  The following network scheduler modules are deprecated:

  - `cls_tcindex`
  - `cls_rsvp`
  - `sch_dsmark`

  - `sch_atm`
  - `sch_cbq`

These modules might be disabled or blocklisted and can be removed in a future release of UEK. The modules are already removed in the upstream Linux kernel.

3 Known Issues

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

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)

4
List of CVEs fixed in this release

The following list describes the CVEs that are fixed in UEK R7U2 (5.15.0-200.131.27) as compared to initial release of UEK R7U1 (5.15.0-100.96.32). 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's critical that you keep your system up-to-date with the latest package updates for this kernel release. Many of the issues listed here might have already been resolved in prior errata builds for the previous update level.

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

- **CVE-2021-4002**

  A memory leak flaw in the Linux kernel's hugetlbfs memory usage was found in the way the user maps some regions of memory twice using shmget() which are aligned to PUD alignment with the fault of some of the memory pages. A local user could use this flaw to get unauthorized access to some data.

  See https://linux.oracle.com/cve/CVE-2021-4002.html for more information.

- **CVE-2022-1679**

  A use-after-free flaw was found in the Linux kernel';s Atheros wireless adapter driver in the way a user forces the ath9k_htc_wait_for_target function to fail with some input messages. This flaw allows a local user to crash or potentially escalate their privileges on the system.

  See https://linux.oracle.com/cve/CVE-2022-1679.html for more information.

- **CVE-2022-3524**

  A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function ipv6_renew_options of the component IPv6 Handler. The manipulation leads to memory leak. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211021 was assigned to this vulnerability.

  See https://linux.oracle.com/cve/CVE-2022-3524.html for more information.

- **CVE-2022-3543**

  A vulnerability, which was classified as problematic, has been found in Linux Kernel. This issue affects the function unix_sock_destructor/unix_release_sock of the file net/unix/af_unix.c of the component BPF. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211043.

- **CVE-2022-3707**

  A double-free memory flaw was found in the Linux kernel. The Intel GVT-g graphics driver triggers VGA card system resource overload, causing a fail in the intel_gvt_dma_map_guest_page function. This issue could allow a local user to crash the system.

  See https://linux.oracle.com/cve/CVE-2022-3707.html for more information.

- **CVE-2022-4379**

  A use-after-free vulnerability was found in __nfs42_ssc_open() in fs/nfs/nfs4file.c in the Linux kernel. This flaw allows an attacker to conduct a remote denial

  See https://linux.oracle.com/cve/CVE-2022-4379.html for more information.

- **CVE-2023-0461**

  There is a use-after-free vulnerability in the Linux Kernel which can be exploited to achieve local privilege escalation. To reach the vulnerability kernel configuration flag CONFIG_TLS or CONFIG_XFRM_ESPINTCP has to be configured, but the operation does not require any privilege. There is a use-after-free bug of icsk_ulp_data of a struct inet_connection_sock. When CONFIG_TLS is enabled, user can install a tls context (struct tls_context) on a connected tcp socket. The context is not cleared if this socket is disconnected and reused as a listener. If a new socket is created from the listener, the context is inherited and vulnerable. The setsockopt TCP_ULP operation does not require any privilege. We recommend upgrading past commit 2c02d41d71f90a5168391b6a5f2954112ba2307c

  See https://linux.oracle.com/cve/CVE-2023-0461.html for more information.

- **CVE-2023-1073**

  A memory corruption flaw was found in the Linux kernel';s human interface device (HID) subsystem in how a user inserts a malicious USB device. This flaw allows a local user to crash or potentially escalate their privileges on the system.

  See https://linux.oracle.com/cve/CVE-2023-1073.html for more information.

- **CVE-2023-1074**

  A memory leak flaw was found in the Linux kernel's Stream Control Transmission Protocol. This issue may occur when a user starts a malicious networking service and someone connects to this service. This could allow a local user to starve resources, causing a denial of service.

  See https://linux.oracle.com/cve/CVE-2023-1074.html for more information.

- **CVE-2023-1079**

  A flaw was found in the Linux kernel. A use-after-free may be triggered in asus_kbd_backlight_set when plugging/disconnecting in a malicious USB device, which advertises itself as an Asus device. Similarly to the previous known CVE-2023-25012, but in asus devices, the work_struct may be scheduled by the LED controller while the device is disconnecting, triggering a use-after-free on the struct asus_kbd_leds *led structure. A malicious USB device may exploit the issue to cause memory corruption with controlled data.

- **CVE-2023-1095**

  In nf_tables_updtable, if nf_tables_table_enable returns an error, nft_trans_destroy is called to free the transaction object. nft_trans_destroy() calls list_del(), but the transaction was never placed on a list -- the list head is all zeroes, this results in a NULL pointer dereference.

  See https://linux.oracle.com/cve/CVE-2023-1095.html for more information.

- **CVE-2023-1118**

  A flaw use after free in the Linux kernel integrated infrared receiver/transceiver driver was found in the way user detaching rc device. 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-2023-1118.html for more information.

- **CVE-2023-20588**

  A division-by-zero error on some AMD processors can potentially return speculative data resulting in loss of confidentiality.

  See https://linux.oracle.com/cve/CVE-2023-20588.html for more information.

- **CVE-2023-22024**

  In the Unbreakable Enterprise Kernel (UEK), the RDS module in UEK has two setsockopt(2) options, RDS_CONN_RESET and RDS6_CONN_RESET, that are not re-entrant. A malicious local user with CAP_NET_ADMIN can use this to crash the kernel. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

  See https://linux.oracle.com/cve/CVE-2023-22024.html for more information.

- **CVE-2023-22998**

  In the Linux kernel before 6.0.3, drivers/gpu/drm/virtio/virtgpu_object.c misinterprets the drm_gem_shmem_get_sg_table return value (expects it to be NULL in the error case, whereas it is actually an error pointer).

- **CVE-2023-22999**

  In the Linux kernel before 5.16.3, drivers/usb/dwc3/dwc3-qcom.c misinterprets the dwc3_qcom_create_urs_usb_platdev return value (expects it to be NULL in the error case, whereas it is actually an error pointer).

- **CVE-2023-23004**

  In the Linux kernel before 5.19, drivers/gpu/drm/arm/malidp_planes.c misinterprets the get_sg_table return value (expects it to be NULL in the error case, whereas it is actually an error pointer).

- **CVE-2023-26545**

  In the Linux kernel before 6.1.13, there is a double free in net/mpls/af_mpls.c upon an allocation failure (for registering the sysctl table under a new location) during the renaming of a device.

  See https://linux.oracle.com/cve/CVE-2023-26545.html for more information.

- **CVE-2023-30456**

  An issue was discovered in arch/x86/kvm/vmx/nested.c in the Linux kernel before 6.2.8. nVMX on x86_64 lacks consistency checks for CR0 and CR4.

  See https://linux.oracle.com/cve/CVE-2023-30456.html for more information.

- **CVE-2023-32233**

  In the Linux kernel through 6.3.1, a use-after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled.

  See https://linux.oracle.com/cve/CVE-2023-32233.html for more information.

- **CVE-2023-42753**

  An array indexing vulnerability was found in the netfilter subsystem of the Linux kernel. A missing macro could lead to a miscalculation of the `h->nets` array offset, providing attackers with the primitive to arbitrarily increment/decrement a memory buffer out-of-bound. This issue may allow a local user to crash the system or potentially escalate their privileges on the system.

See https://linux.oracle.com/cve/CVE-2023-42753.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
```