# Notice Description

The Oracle Linux UEFI Secure Boot Signing Key Update Notices provides information about updates to the Unified Extensible Firmware Interface (UEFI) Secure Boot signing keys used by Oracle to sign kernels and related packages that are used for UEFI Secure Boot.

## Notices

A system in UEFI Secure Boot mode only loads boot loaders and kernels that have been signed by Oracle. Oracle updates the kernel and grub2 packages to sign them with a valid Extended Validation (EV) certificate in the event that a key may expire or for additional security updates. The EV certificate is compiled into the shim binary and is signed by Microsoft. This feature is fully supported from Oracle Linux 7.3 onward.

All kernels and affected packages that were released previously should continue to work at their current version. However, if you intend to update a kernel or packages, these notices apply; you should perform an atomic update in accordance with the instructions provided here.

The information in this document describes events where the kernels and associated packages are updated with new keys. Each section describes the minimum kernel versions that are affected by the change and the package versions that have been updated with the new keys.

## [2023-03-09] Improved Key Revocation Process to Mitigate UEFI Secure Boot CVEs: CVE-2022-3775, CVE-2022-2601

Oracle now uses UEFI Secure Boot Advanced Targeting (SBAT) to revoke core boot components as a mitigation for CVE-2022-3775 and CVE-2022-2601. This update affects users of Oracle Linux 8 and Oracle Linux 9.

The `grub2` and `shim` packages listed contain UEFI binaries with their revocation level set to "3" in the `.sbat` section of their metadata. Oracle can increment those values asynchronously as required.

For more information about using `mokutil` to verify and configure SBAT policies when UEFI Secure Boot is enabled, see Oracle Linux: Working With UEFI Secure Boot.

### Oracle Linux 9

On Oracle Linux 9, following package versions introduce UEFI SBAT metadata for key revocation:

- **grub2**

  v2.06-46.0.4.el9
- **shim-x64**

  v15.7-1.0.3.el9

### Oracle Linux 8

On Oracle Linux 8, following package versions introduce UEFI SBAT metadata for key revocation:

- **grub2**

  v2.02-142.0.3.el8_7.1
- **shim-x64**

  v15.7-1.0.3.el8

## [2022-06-14] Keys Update for UEFI Secure Boot CVEs: CVE-2021-3695, CVE-2022-28737, CVE-2022-21499

Oracle has rotated the UEFI Secure Boot signing certificates that are used to sign Oracle Linux kernels in response to CVE-2022-21499, grub2 instances in response to CVE-2021-3695 and also shim binaries in response to CVE-2022-28737. This update affects users who are running Oracle Linux 7 and Oracle Linux 8.

Additional vulnerabilities that have been patched as part of this update include the following for grub2:

- CVE-2021-3695
- CVE-2021-3696
- CVE-2021-3697
- CVE-2022-28733
- CVE-2022-28734
- CVE-2022-28735
- CVE-2022-28736

Newer kernel versions are signed with the new key and provide the "`oracle(kernel-sig-key)=202204`" functionality that is required for the new shim. Other components must be updated in the same atomic operation if you upgrade the system.

> **Important:**
>
> The Red Hat Compatible Kernel (RHCK) requires additional security fixes for CVE-2022-21499 so that Oracle Linux can load RHCK with UEFI Secure Boot enabled. For more information, see Enabling RHCK With Additional Security Fixes From Oracle.

## Oracle Linux 7

On Oracle Linux 7, the following kernel package versions, or higher, are signed with the new key:

- **Red Hat Compatible Kernel (RHCK)**

  v3.10.0-1160.66.1.0.2
- **Unbreakable Enterprise Kernel Release 4 (UEK R4)**

  v4.1.12-124.63.2.1
- **Unbreakable Enterprise Kernel Release 5 (UEK R5)**

  v4.14.35-2047.513.2.3
- **Unbreakable Enterprise Kernel Release 6 (UEK R6)**

  v5.4.17-2136.307.3.6

The following package versions are also signed with compatible new certificates:

- **grub2**

  v2.02-0.87.0.21.el7_9.9 (Required)
- **shim-x64**

  v15.6-1.0.7.el7 (Required)

## Oracle Linux 8

On Oracle Linux 8, the following kernel package versions, or higher, are signed with the new key:

- **Red Hat Compatible Kernel (RHCK)**

  v4.18.0-372.9.1.0.2
- **Unbreakable Enterprise Kernel Release 6 (UEK R6)**

  v5.4.17-2136.307.3.6
- **Unbreakable Enterprise Kernel Release 7 (UEK R7)**

  v5.15.0-0.30.19

The following package versions are also signed with compatible new certificates:

- **grub2**

v2.02-123.0.3.el8 (Required)

- **shim-x64**

  v15.6-1.0.3.el8 (Required)

## [2020-07-29] Key Update for CVE-2020-10713

Oracle has updated the key that it uses to sign UEK kernels and grub instances in response to CVE-2020-10713. This update affects users who are running Oracle Linux 7 and Oracle Linux 8.

Newer kernel versions are signed with the new key and require that other components are updated as an atomic operation if you upgrade the system.

### Oracle Linux 7

On Oracle Linux 7, the following kernel package versions, or higher, are signed with the new key:

- **Red Hat Compatible Kernel (RHCK)**

  v3.10.0-1127.18.2

- **Unbreakable Enterprise Kernel Release 3 (UEK R3)**

  v3.8.13-118.47.2

- **Unbreakable Enterprise Kernel Release 4 (UEK R4)**

  v4.1.12-124.40.6.3

- **Unbreakable Enterprise Kernel Release 5 (UEK R5)**

  v4.14.35-1902.304.6.3

- **Unbreakable Enterprise Kernel Release 6 (UEK R6)**

  v5.4.17-2011.4.6

The following package versions are signed with the same EV certificate as the latest kernel releases:

- **`grub2`**

  v2.02-0.82.0.5 (required)

- **`shim-x64`**

  v15-2.0.5 (required)

- **`fwupdate-efi`**

  v12-5.0.5 (optional)

### Oracle Linux 8

On Oracle Linux 8, the following kernel package versions, or higher, are signed with the new key:

- **Red Hat Compatible Kernel (RHCK)**

  v4.18.0-193.14.3
- **Unbreakable Enterprise Kernel Release 6 (UEK R6)**

  v5.4.17-2011.4.6

The following package versions are signed with the same EV certificate as the latest kernel releases:

- **`grub2`**

  v2.02-82.0.2 (required)
- **`shim-x64`**

  v15-11.0.5 (required)
- **`fwupdate-efi`**

  v11-3.0.3.el8 (optional)
- **`fwupd`**

  v1.1.4-6.0.2.el8 (optional)

## [2018-11-15] Key Expiry Update

Oracle has updated the key that it uses to sign kernels and grub instances to avoid key expiry. This update affects users who are running Oracle Linux 7 and Oracle Linux 8.

Newer kernel versions are signed with the new key and require that other components are updated as an atomic operation if you upgrade the system .

The update affects all UEK releases, as well as RHCK. The following kernel package versions, or higher, are signed with the new key:

- **Red Hat Compatible Kernel (RHCK)**

  v3.10.0-957.0
- **Oracle Modified Red Hat Compatible Kernel (RHCK)**

  v3.10.0-957.0.0.0.2
- **Unbreakable Enterprise Kernel Release 3 (UEK R3)**

  v3.8.13-118.27.1
- **Unbreakable Enterprise Kernel Release 4 (UEK R4)**

  v4.1.12-124.22.1
- **Unbreakable Enterprise Kernel Release 5 (UEK R5)**

  v4.14.35-1818.4.6

The following package versions are signed using the same EV certificate as the latest kernel releases:

- **`grub2`**

v2.02-0.76.0.3 (required)

- **shim-x64**

  v15-1.0.3 (required)

- **fwupdate-efi**

  v12-5.0.3 (optional)

# Handling Kernel Upgrades and Downgrades

If you are using UEFI Secure Boot, you should be aware of the following action items when upgrading or downgrading packages on your system:

## Upgrading Your Kernel

If you have previously enabled Secure Boot and you intend to upgrade your kernel, you must ensure that you update `shim-x64`, `grub2` and `kernel` packages as an atomic operation. If all of these packages are not updated, the Secure Boot process may break and must be disabled until a full system upgrade is complete.

The `fwupdate-efi` package is also affected by this update. Although this package is not essential for boot, you may wish to update it to a version that is equal to or higher than the versions listed below if you have it installed.

If you upgrade your kernel to a version that is equal to, or higher than, a version signed with a new EV certificate, as described in Notices, make sure the associated packages are upgraded to the specified versions or later.

You should pay attention to determine whether the kernel version that you intend to install or upgrade to is affected by a key update and install the appropriate minimum package versions at the same time.

Finally, do not forget to follow the instructions in Rebuilding Your Rescue Kernel.

## Downgrading Your Kernel

If you have enabled Secure Boot, are running a kernel version that is signed with the latest EV certificate, and you intend to downgrade the kernel to a version that is lower than any of those that are listed in Notices, you must downgrade the `shim-x64`, `grub2` and `kernel` packages as an atomic operation. Ensure that the `shim` and `grub2` packages are *lower* than the versions listed in Notices.

You should pay attention to determine whether the kernel version that you intend to downgrade to is affected by an alternate key update and install the appropriate package versions at the same time.

Finally, do not forget to follow the instructions in Rebuilding Your Rescue Kernel.

## Rebuilding Your Rescue Kernel

Whenever you upgrade or downgrade packages with new signatures for use with UEFI Secure Boot, you must rebuild your system rescue kernels to maintain the ability to boot into those environment whenever that is required.

Remove any old rescue kernels that have been signed with the previous EV certificate:

```
sudo rm -f /boot/initramfs-0-rescue-*

sudo rm -f /boot/i/boot/vmlinuz-0-rescue-*
```

Generate new rescue kernels that have been signed with the current EV certificate:

```
sudo /etc/kernel/postinst.d/51-dracut-rescue-postinst.sh $(uname -r) /boot/
vmlinuz-$(uname -r)
```

## Enabling RHCK With Additional Security Fixes From Oracle

Oracle maintains strict security requirements when signing kernels and packages for use with UEFI Secure Boot, particularly when that is necessary for urgent security issues and CVEs.

You can safely boot Oracle Linux and RHCK when UEFI Secure Boot is enabled. The series of CVEs listed in [2022-06-14] Keys Update for UEFI Secure Boot CVEs: CVE-2021-3695, CVE-2022-28737, CVE-2022-21499 required Oracle to rotate the current certificates with new certificates, which prevents kernels signed with older certificates from loading. Due to the importance of CVE-2022-21499, Oracle has applied the necessary fix to both UEK and RHCK. Customers using UEFI Secure Boot with RHCK must apply the modified RHCK errata by using the following instructions:

### Oracle Linux 7

Enable the `ol7_MODRHCK` software channel:

```
sudo yum-config-manager --enable ol7_MODRHCK
```

Update your system to install the latest RHCK release with additional security fixes:

```
sudo yum update -y
```

You can safely leave the `ol7_MODRHCK` channel enabled, as the latest RHCK release is always installed during an update. To optionally disable the `ol7_MODRHCK` channel, run the following command:

```
sudo yum-config-manager --disable ol7_MODRHCK
```

### Oracle Linux 8

Update the `oraclelinux-release-el8` package, then enable the `ol8_MODRHCK` software channel:

```
sudo dnf update oraclelinux-release-el8

sudo dnf config-manager --enable ol8_MODRHCK
```

Update your system to install the latest RHCK release with additional security fixes:

```
sudo dnf update -y
```

You can safely leave the `ol8_MODRHCK` channel enabled, as the latest RHCK release is always installed during an update. To optionally disable the `ol8_MODRHCK` channel, run the following command:

```
sudo dnf config-manager --disable ol8_MODRHCK
```

---

Oracle Linux UEFI Secure Boot Update Notices
F12070-13