

Oracle® Linux
UEFI Secure Boot Signing Key Update Notice

ORACLE®

F12070-02
September 2019

Oracle Legal Notices

Copyright © 2019, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Abstract

This document contains information about an update to the UEFI Secure Boot signing key used by Oracle to sign kernels and grub packages released by Oracle. This update affects users of both the Unbreakable Enterprise Kernel and Red Hat Compatible Kernel (RHCK) on systems that are configured for UEFI Secure Boot. This document may be updated after it is released. To check for updates to this document, and to view other Oracle documentation, refer to the Documentation section on the Oracle Technology Network (OTN) Web site:

<https://docs.oracle.com/en/operating-systems/linux.html>

This document is intended for users and administrators of Oracle Linux. It describes an update to the UEFI Secure Boot signing key used by Oracle to sign kernels and grub packages released by Oracle. This update affects users of both the Unbreakable Enterprise Kernel and Red Hat Compatible Kernel (RHCK) on systems that are configured for UEFI Secure Boot. It provides instructions on how to update your system if you are using UEFI Secure Boot and how to handle a downgrade in the event that you need to use a kernel signed by an earlier signing key. Oracle recommends that you read this document before upgrading or downgrading your kernel if you use UEFI Secure Boot.

Document generated on: 2019-09-05 (revision: 8257)

Table of Contents

Preface	v
1 Notice Description	1
2 Action Items	3
2.1 Upgrading	3
2.2 Downgrading	3

Preface

The *Oracle Linux UEFI Secure Boot Signing Key Update Notice* provides information about an update to The UEFI Secure Boot signing key used by Oracle to sign kernels and related packages that are used for UEFI Secure Boot.

Audience

This document is written for system administrators who want to use UEFI Secure Boot with Oracle Linux. It is assumed that readers have a general understanding of the Linux operating system.

Related Documents

The latest version of this document and other documentation for this product are available at:

<https://docs.oracle.com/en/operating-systems/linux.html>.

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1 Notice Description

Oracle has updated the key that it uses to sign kernels and grub instances to avoid key expiry. A system in Secure Boot mode will load only boot loaders and kernels that have been signed by Oracle. Oracle has updated the kernel and grub2 packages to sign them with a valid Extended Validation (EV) certificate. The EV certificate has been compiled into the shim binary and has been signed by Microsoft. This feature is fully supported from Oracle Linux 7 Update 3 onward.

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 the 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

All kernels and affected packages released previously should continue to work at their current version.

Chapter 2 Action Items

Table of Contents

2.1 Upgrading	3
2.2 Downgrading	3

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

2.1 Upgrading

If you have previously enabled Secure Boot and you intend to upgrade your kernel, you must ensure that you update `shim`, `grub2` and `kernel` packages as an atomic operation. If these packages are not all 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 the new EV certificate, as described in [Chapter 1, Notice Description](#), make sure the following packages are upgraded to the specified versions or later:

- `grub2.` v2.02-0.76.0.3 (required)
- `shim.` v15-1.0.3 (required)
- `fwupdate-efi.` v12-5.0.3 (optional)

The package versions listed above are signed using the same EV certificate as the latest kernel releases.

2.2 Downgrading

If you have enabled Secure Boot, are running a current kernel version signed with the latest EV certificate, and you intend to downgrade kernel to a version lower than any listed in [Chapter 1, Notice Description](#); you must downgrade the `shim`, `grub2` and `kernel` packages as an atomic operation. Ensure that the `shim` and `grub2` packages are *lower* than the versions listed in [Section 2.1, "Upgrading"](#).
