THALES

CipherTrust Transparent Encryption for Linux

Release Notes

- **Release 7.5.0.78**
- **Date: December 19, 2023**
- **Document Version: 1**

New Features and Enhancements

Release 7.5.0.78 of CipherTrust Transparent Encryption (CTE) for Linux adds new features, fixes known defects, and addresses known vulnerabilities.

Curl CLI Tool

- Curl v8.4.0 is now supported.

New Platform Support

The following kernels are supported starting with the CTE v7.4.0 GA release:

RHEL

- **RHEL 8.9**
- **RHEL 9.3**

Ubuntu

- **Ubuntu 22.04.2 with kernel 5.19 kernel**

Secure Boot Advisory

For CipherTrust Transparent Encryption to support Secure Boot, the signing key for CTE kernel modules must be renewed every three years. Thales' current schedule for changing the signing key is the first week of 2024. For customers who take advantage of Secure Boot with CTE, the new certificate, matching the new signing key, must be added to their systems by the end of this year 2023 to ensure a smooth upgrade. In CTE 7.5, Thales will provide instructions for obtaining the new certificate.

Operating Support Advisory

This advisory covers changes planned for Operating System and Linux kernel support with CTE 7.5.0 scheduled to release in December 2023.

1. Windows Server 2012 and 2012 R2 are reaching End-of-Life. Microsoft will no longer support them. Thales CTE 7.5.0 will also drop support for those operating systems.

2. RHEL 7 reaches End-of-Support with CTE 7.5.0.

3. Red Hat Enterprise Linux (RHEL) new major and minor release SLA changes as follows.
   - * Major: 60 Business Days
   - * Minor/Service Pack: 30 Business Days

   > **Note:** There is **NO** change to **critical** kernel security patch SLA. Thales continues to support four business days. {.note}

4. Ending support for older Linux kernels as per the following table:

Operating System	Last supported CTE release
RHEL 7.5 - RHEL 7.9	7.4.0.x
RHEL 8.0 - RHEL 8.6	7.4.0.x
SLES-12 SP3 (all default kernels and up-to kernel 4.4.140-96.112.TDC-default for Teradata)	7.4.0.x
SLES-12 SP4 (4.12.14-94.41-default to 4.12.14-95.54-default)	7.4.0.x
SLES-12 SP4 (4.12.14-94.41-default to 4.12.14-95.54-default)	7.4.0.x
SLES-12 SP5 (4.12.14-120-default to 4.12.14-122.63-default)	7.4.0.x
SLES-15 SP0 to SLES 15 SP3	7.4.0.x

End of Life

- CipherTrust Transparent Encryption v7.5 and subsequent versions no longer support CTE-Efficient Storage for Linux.

- Ubuntu 18.04 is no longer supported

Sales and Support

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

For support and troubleshooting issues:

- https://supportportal.thalesgroup.com
- (800) 545-6608

For Thales Sales:

- https://cpl.thalesgroup.com/encryption/contact-us
- CPL_Sales_AMS_TG@thalesgroup.com
- (888) 267-3732

Notices and License

All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries and affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

- This document shall not be posted on any publicly accessible network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.