CipherTrust Transparent Encryption (CTE) for Linux

Release Notes

- **Release: 7.1.0.66**
- **Date: March 23, 2021**

New Features and Enhancements

Release 7.1.0.66 of CipherTrust Transparent Encryption (CTE) for Linux adds new features, fixes known defects, and addresses known vulnerabilities.

The major improvements to CTE for Linux in this release are:

- CTE-Live Data Transformation now supports creating CTE-LDT GuardPoints on Linux NFS shares if you are using the Vormetric Data Security Manager (DSM) as your key manager. For details, see *CTE-Live Data Transformation with Data Security Manager*.

  > **Note:** If any files are opened exclusively by another application on an NFS/CIFS share, CTE-LDT cannot rekey those files until the other applications have released the lock.

  > **Note: Snapshot directories over NAS volumes using NFS:** Thales requires disabling snapshots on directories guarded with a GuardPoint on a CTE host using LDT policies. You can use snapshots to restore volumes or individual files, however, using snapshots with LDT is not recommended, especially during active live data transformation, due to the continuous changes to the data in files and the LDT metadata for files during rekey. LDT partitions files in small chunks for rekey. Each chunk is rekeyed separately, and the data undergoing rekey is saved in MDS along with corresponding metadata before the data is encrypted and rewritten to the target file. As LDT does not rekey the entire contents of a file in a single operation, snapshots of files created during rekey are not usable after rekey completion. A file snapshot might have a mix of data encrypted with two keys, or clear-text during initial transformation, without the availability of corresponding metadata required for accessing the data. Therefore, using local snapshots on GuardPoints over NAS volumes using NFS is not recommended.

- Linux installation with UEFI Secure Boot is now available. For details, see the *CTE Agent for Linux Advanced Configuration and Integration Guide*.

New Platform Support

- Ubuntu 20.04
  - 5.8.0-29-generic
  - 5.8.0-33-generic
  - 5.8.0-36-generic
  - 5.8.0-38-generic
  - 5.8.0-40-generic
  - 5.8.0-41-generic
- Ubuntu 20.04.2
  - 5.8.0-43-generic

Documentation Enhancements

- All CTE documentation is available at https://thalesdocs.com/ctp/cte/index.html.
- The CTE Compatibility Portal is now online.

  > **Note:** The portal works best with Firefox and Chrome.

Resolved Issues

- **AGT-29358: DD cmd does not fail properly on IDT device when device has reservation restrictions on write**

  When running on a Linux kernel version >= 4.4, guarded raw devices (SECVM) may not accurately propagate real errors from the underlying disk back up for the user space application. With this fix, all errors are properly sent back to the caller.
- **AGT-29578: VTE uninstall leaves COS files behind**

  When CTE with COS enabled, was uninstalled, a CTE COS related directory remained. This has been fixed.
- **AGT-29836 [CS1004828]: db2sysc denied following DSM upgrade**

  Caused by a race condition between two db2 bp processes. This has been fixed.
- **AGT-29909 [CS1006174]: Receiving kernel errors for multiple servers. Red Hat analysis points to secfs2.**

  After upgrading CTE, restart CTE.
- **AGT-29962: Failed to disabled unit msg during DSM registration on RHEL8u2**

  If the cos S3 service is not enabled, during registration, the registration script will check for an installed Squid Proxy service before doing a systemctl/systemd disable. If the Squid Proxy is not installed, there is no need for the registration script to do systemctl disable operation

  This issue has been fixed in this release of the CTE Agent.
- **AGT-30032 [CS1003860]: Prevent non root user from invoking squid and hardening the file access permissions**

  The squid proxy service is now only started when COS is enabled.

- **AGT-30608 [CS1020770]: Vormetric processes causing slowdown on production database (100% CPU)**

  VTE Linux by default no longer uses the vmap mode of Linux kernel virtual memory addressing. This eliminates holding certain virtual memory related locks.

- **AGT-31116: In ESG, added a command to display if XTS key is supported**

  Added: `# voradmin secfs status crypto`

- **AGT-31338 [CS1028087]: VMD triggered the system crash**

  Crash was caused by system not receiving proper credentials. The credentials are now restored properly.

- **AGT-31378 [CS1030945]: GuardPoints failed to guard after a system rebooted**

  The system access file was corrupted. This has been fixed.

- **AGT-31792: Disable a GuardPoint that is rekeying with a prior version**

  In 7.1.0, if a GuardPoint is rekeying with a prior version, it will be disabled in 7.1.0. This restriction will be relaxed in 7.1.1.

Known Issues

- **AGT-30185: Failed to backup ::vorm:ldtxattr:: in LDT over NFS GuardPoint due to restricted permissions**

  In version 7.1.0, NFS GuardPoints must be backed up using tar.

- **AGT-31897: Manually unguarding an ESG or IDT-Capable device that failed transformation displays an error message**

  An ESG or IDT-Capable device guarded with a manual GuardPoint does not get disabled when the device has failed to complete data transformation. Instead, the error message seen in 'secfsd -status guard' output is repeated in the output of the secfsd unguard command.

  Workaround: Wait approximately 30 seconds for CTE to automatically attempt another unguard operation. The ESG or IDT-Capable device should be successfully unguard on the second attempt. This issue will be fixed in a subsequent release.

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 DIS France S.A. and/or its subsidiaries or 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 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.