CipherTrust Transparent Encryption (CTE) for Linux

Release Notes

- **Release: 7.1.1.30**
- **Date: July 08, 2021**

New Features and Enhancements

Release 7.1.1.30 of CipherTrust Transparent Encryption (CTE) for Linux adds new features, fixes known defects, and addresses known vulnerabilities.

- **Enhanced Host Setting**

  Supports |path_no_trust| when |trust|* is also defined

- **LDT**

  Ability to rename directories inside an LDT GuardPoint

- **Efficient Storage GuardPoints**

  Supports migration of a Standard Policy GuardPoint to an Efficient Storage GuardPoint

- **DSM to CM communication**

  Enhance CTE Challenge/ Response to return an error after wait timeout with DSM, CipherTrust Manager communication

- **Anti-virus support**

  Support for Sentinel One AV

  Support for McAfee 10.7.x

CipherTrust Intelligent Remediation support with Standard and LDT policies

CipherTrust Intelligent Remediation enables organizations to assess all of their data, discover and protect sensitive data, and classify data according to various data privacy laws, by using the CipherTrust Intelligent Remediation solution with CipherTrust Data Discovery and Classification for finding and classifying sensitive

data, and CipherTrust Transparent Encryption for encrypting that data. This protects customer data, achieves compliance, and best practice requirements. It helps a company avoid devastating financial, legal and reputational consequences that can occur if an organization's network is breached and sensitive data is stolen.

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-31806 [CS1038224]: VTE Agent not validating the DSM certificate**

  Due to an error in the runtime engine used to perform encrypted communications with the server, certificate peer verification was inadvertently disabled, resulting in this vulnerability. That error is corrected with this fix.

- **AGT-32493: Problems with restoring full backup image of a GuardPoint**

  At the time, CTE-LDT does not support restoring a full backup image of a GuardPoint when the target GuardPoint is partially rekeyed. To restore the backup, you must first remove all of the files, including the MDS file, in the target GuardPoint directory before restoring the backup image. Run the voradmin command to remove the MDS file from the GuardPoint directory.

- **AGT-33312 [CS1053894]: X-form Percentage is missing in Rekey status on DSM Wen UI**

  Starting with this release of CTE, DSM continues displaying the percentage of data rekeyed through LDT on the DSM's GuardPoints page for a host. With this change, DSM displays the primary/non-primary status of the host for the GuardPoints over NFS in the GuardPoint Status pop-up window.

- **AGT-33314 [CS1055579]: secfs-fs-barrier.service fails to start on CTE 7.1.0.66 or above**

  See AGT-33407.

- **AGT-33407 [CS1056060]: SecFS-fs is not starting after agent upgrade**

  The issue causes the following messages to appear in the **`systemctl -l status secfs-fs`** output on CTE v7.1.0.

  ```
  /opt/vormetric/DataSecurityExpert/agent/secfs/bin/secfs-systemd-helper: line 1279:
  [: too many arguments
  ```

  ```
  /opt/vormetric/DataSecurityExpert/agent/secfs/bin/secfs-systemd-helper: line 1284:
  [: too many arguments
  ```

  This happens when ORACLE is installed, but ORACLE_BASE is not defined in `.bash_profile`. A bug in the CTE startup script caused this message to appear in such a scenario. The script has been fixed to handle this condition in 7.1.1.

  Note: This message does not cause a failure for the secfs-fs service startup. On CTE 7.1.0, those messages can be avoided by using the following workaround:

  1. Ensure that the ORACLE_BASE variable is assigned a value in `/root/.bash_profile`.
  2. Ensure that a line starting with +ASM exists in the `/etc/oratab`. This line is added by the Oracle installer when Oracle is configured with ASM.

- **AGT-33413: CM Domain names contain space, CTE needs to accommodate**

  The CM domain name can include spaces. However, Syslog does not allow spaces in header fields. Therefore, for Syslog purposes, the CTE client replaces the spaces with an underscore. For example: My_ Domain instead of My Domain.

Known Issues

CTE

- **AGT-33410 [CS1055172]: Received permission denied when trying to append a file on NFSv4**

  The problem is related to user permissions, for non-root users, from the RHEL 8.3 and 8.4 kernels. This will be fixed in a future patch.

CipherTrust Intelligent Remediation

- **KY-27653: Changing PQS Schema**

  Thales does not support changing schemas in this release of CipherTrust Intelligent Remediation. Changing the PQS schema can corrupt data because GuardPoints do not migrate properly from the old schema to the new schema.

- **KY-30508: Rotating the LDT Key version for a CBC-CS1 key during the remediation of files hangs the Kernel and stops the remediation**

  Defer LDT key rotation for those keys applied on GuardPoints that are undergoing remediation on Redhat 7.x. Check the remediation report for those GuardPoints to confirm that all sensitive files are encrypted before rotating the relevant CBC-CS1 keys.

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

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.