PKWARE® z/OS® HIPER Notification

HIPER ID: V10TT5482

Announced: July 21, 2009

Affected Products:

SecureZIP® for z/OS® v10.0 Standard Edition
SecureZIP for z/OS v10.0 Enterprise Edition
SecureZIP Partner for z/OS 10.0

Affected Feature:

Encryption/Decryption using ICSF IBM_HARDWARE with a PCIXCC or CEX2C cryptographic processor.

Required ZIP Processing Parameters:

```
FIPSMODE (any active 140 value)
ENCRYPTION_METHOD (DES,3DES, or AESnnn on qualified system
z9 or z10 systems)
```

Notification Details:

The PKWARE z/OS Quality Assurance team has identified a possible processing impact when implementing ICSF at a minimum release of HCR7751. Activation of CKDS Key Store Policy checking with CLASS(XFACILIT) may result in Security Server violations for CLASS(CSFKEYS) when attempting SecureZIP cryptographic operations using secure keys. Such violations will cause SecureZIP operations to fail unless administrative action is taken.

ICSF HCR7751 is the default level distributed with z/OS 1.10, but may be installed on earlier supported releases of z/OS. The documentation associated with Key Store Policy checking is documented in the IBM z/OS 1.10 ICSF Administrator's Guide SA22-7521-13; "Controlling Who Can Use Cryptographic Keys and Services."

Qualified System z9 systems with a CEX2C MCL upgrade to enable secure key AES operations are affected in the same way as System z10 environments.

It is assumed that the installation's security plan provides direction for the implementation of ICSF key store policy checking. Only those features having a particular influence on SecureZIP operations are identified in this document. Please consult with your ICSF and Security Server administrator for details regarding the activation of ICSF resource controls at your installation.

Overview:

Administrative actions may differ depending on the system configuration and processing options chosen. Please review the entire document to identify all aspects that pertain to your installation.

ICSF performs Security Server resource checks for specific services requested. This affects the following aspects of SecureZIP cryptographic operations:

- (SecureZIP – all listed releases)

  ICSF CKDS key store policy checking for keys not found to be registered in the CKDS fall into a “default” category of keys to prevent unregistered key usage. This mode is activated by CLASS(XFACILIT) CSF.CKDS.TOKEN.CHECK.DEFAULT.LABEL. Once activated, ICSF performs a security server check against CLASS(CSFKEYS) CSF-CKDS-DEFAULT. Some ICSF services not directly involved with CKDS processing may be affected.

  Action Required: The following SecureZIP cryptographic features require that READ permission be granted to the CSF-CKDS-DEFAULT resource in CLASS(CSFKEYS):

  - Encryption/Decryption with –RECIPIENT.
  - Encryption/Decryption with –PASSWORD, with either CKDS label/title designations, or passphrase value (all releases).

  ICSF symmetric key processing requests will fail with Return Code=0008, Reason Code=3064 if permission is not granted.

  The ICSF Administrator's Guide has information about placing the key store policy and the associated resource into WARN mode. This provides an opportunity to identify processes that may be adversely affected by running in FAIL mode. Consult with the installation Security Administrator to determine best practices at your installation.

CA-ACF2® Special Requirement: This security server may be automatically enabling ICSF CKDS Key Store Policy checking unless maintenance is applied. Consult with your Computer Associates support service and reference ++APAR(TA8654B).

See the ICSF started task log for the following message:

```
CSFM608I A CKDS KEY STORE POLICY IS DEFINED.
```

```
++APAR(TA8654B) /* CA ACF2 r12    */

   STARTRAK PROBLEM: 8654
   ABSTRACT: ICSF XFACILIT EXTRACT ALWAYS GETS RC 0

   DESCRIPTION:

      RACROUTE EXTRACT calls for entities in the XFACILIT class
      erroneously set return and reason code zero. The calls are
      issued when CSF comes up if the HCR7751 version of ICSF is
      being used.
```

CA-Top Secret Security® Special Requirement: ICSF looks for a CSF-CKDS-DEFAULT resource in the CSFKEYS class to determine application access. However, CA-Top Secret Security does not support hyphens “-“ in a resource name.

```
TSS0240E  INVALID RESOURCE NAME
```

Therefore, masking characters may be used in their place:

```
TSS PERMIT(...) CSFKEYS(CSF+CKDS+DEFAULT) ACCESS(READ)
```

Contact PKWARE: If additional information is required regarding this announcement, please contact the PKWARE Support team at +1.937.847.2687 (option 2).