Driver 41 Customer Exception Letter

Level 00i - 24 May 2023

z15 (MT 8561, MT 8562)

SC28-7001-00

This edition, SC28-7001-00i, applies to IBM z15 (z15) processors, Driver 41. This version replaces SC28-7001-00h, SC28-7001-00g, SC28-7001-00f, SC28-7001-00e, SC28-7001-00d, SC28-7001-00c, SC28-7001-00b, SC28-7001-00a and SC28-7001-00.

There might be a newer version of this document in a **PDF** file available on **Resource Link**, go to http://www.ibm.com/servers/resourcelink. A newer version is indicated by a lowercase, alphabetic letter following the form number suffix (for example: 00a, 00b, 01a, 01b).

© Copyright International Business Machines Corporation 2019, 2023.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this Customer Exception letter

This exception letter is used by a customer and should be reviewed in its entirety. It includes information pertaining to the driver, such as:

- Functional exceptions
- Code restrictions
- General information
- Specific customer information

Acquiring the latest version

The latest version of this letter is available in portable document formation (PDF) on **Resource Link®**. Go to http://www.ibm.com/servers/resourcelink, click **Fixes** on the navigation bar, select **Exception letters** located under **Known defects/problems**, select the system and then the driver exception letter you need.

© Copyright IBM Corp. 2019, 2023

Code considerations

September 2020 announce delivery

The September 2020 announce delivery includes the following:

- Enhanced System Recovery Boost capabilities enable customers to use a new class of boost that can be applied to a range of sysplex recovery processes that includes: sysplex partitioning, CF structure recovery, CF data sharing member recovery, and IBM® HyperSwap® recovery.

  Available with the release of Bundle S29, released 30 September 2020.
- Cryptographic enhancements for Common Cryptographic Architecture (CCA) and Enterprise PKCS#11 (EP11) provide increased functionality and security.

  Available with the release of Bundle S30a, released 30 September 2020.

  Attention: Installation of these MCLs will set “Pending Conditions” for Crypto Express7S. This will require a vary offline/online of each Hardware Security Module (HSM) to activate these changes.

  For z/OS® customers, Cryptographic Support for z/OS V2R13 - z/OS V2R4 (HCR77B1) provides helpful commands to interrogate and manage the manual vary off/on tasks. For details, refer to Instructions for non-concurrent Crypto updates while running ICSF .
- Reserved space: Provides additional redundant power ports, weight ballast, and airflow mechanicals. Only available on single frame models T02 and LT2, meeting configuration requirements.

  Available from manufacturing as of 15 September 2020.

The following announcements are exclusive for IBM LinuxONE Models LT1 and LT2:

- NVMe boot support: Initial program load boot support from IBM Adapter for NVMe devices.
- Support of coupling adapters as timing only link for STP (Server Time Protocol) usage.

  Available with the release of Bundle S29, released 30 September 2020.

Fibre Channel endpoint security

This feature delivery has completed an Early Adopter Program (EAP).

The recommended minimum levels are Bundle S29a, released on 15 September 2020. There are also required DDS8000 and SKLM levels.

Secure Execution for Linux on Z

This feature delivery has completed an Early Adopter Program (EAP).

The recommended minimum levels are Bundle S39, released on 22 April 2021.

May 2021 announce delivery

The May 2021 announce delivery includes the following:

- BCPii V2, a new BCPii infrastructure that provides the ability to send REST API information through the z/OS Base Control program.

  The recommended minimum level is Bundle S43 and H27, released 16 June 2021.

© Copyright IBM Corp. 2019, 2023

- LDAP group membership, allows both the HMC and SE users become part of LDAP group membership.

  The recommended minimum level is Bundle S43 and H27, released 16 June 2021.
- DPM has added support for FCP Tape devices.

  The recommended minimum level is Bundle S39a, released on 22 April 2021.
- Remote Code Load, this will support IBM Z® firmware updates without requiring a person to be inside the data center monitoring these planned updates.

  Currently, support levels are provided under an Early Adopter Program (EAP).
- Cryptographic Architecture (CCA) enhancement, the addition of a TDES key block (a key token). This new TDES keyblock uses a new wrapping method that is known as “WRAPENH3”.

  The recommended minimum level is Bundle S39a, released on 22 April 2021.

October 2021 - Stand-alone Coupling Facility firmware update may require z/OS OA59075

Bundle S51a, released 13 October 2021, changed the firmware infrastructure supporting dynamic changes for an IBM z15® (z15) Stand-alone Coupling Facility. This change requires a software PTF / APAR OA59075 to be installed on the CPC that is running z/OS - HCD and driving the hardware only type dynamic changes to the Stand-alone Coupling Facility.

PTF / APAR OA59075 was released in June 2021 and was marked HIPER. The intent was that the PTF would be installed well before the z15 firmware change is installed.

Note: This firmware infrastructure change does not alter customer operations or procedures used for dynamic changes to a Stand-alone Coupling Facility. Bundle S51a can be identified by the installation of MCL002 in the P46613 EC Stream.

Sysplex and STP connectivity information

IBM z15 (z15) machines will continue to follow IBM (n-2) "statement of support" for Parallel Sysplex® server hardware based on connectivity over coupling links or STP timing-only links. z15 STP is only supported for the following IBM Z servers:

- z14 Model ZR1 (3907) at Driver 36
- z14 (3906) at Driver 36
- z13s® (2965) at Driver 27
- z13® (2964) at Driver 27

Recommended coupling facility control code levels

The following MCL and CFCC levels are recommended when coupling with a z15 (MT 8561). Product Engineering (PE) always recommends the highest available MCL level for best performance and availability.

- z13 / z13s (MT 2964 / MT 2965)
  - CFCC Product Release 21 - Service level 2.20

    This can be identified by the Activation of the following MCL:

    - Driver 27 Bundle S82 / MCL P08416.008 (Released February 2019)
- z14 (3906 and 3907)
  - CFCC Product Release 23 - Service level 00.13

    This can be identified by the activation of the following MCL:

    - Driver 36 Bundle S13 / MCL P41419.003 (Released February 2019)

Minimum firmware levels for MT 8561

The Minimum Ship Level (MSL) firmware for September 2019 shipments is defined as Bundle S04c.

Additional firmware updates were released after shipments that include important stability and serviceability improvements.

Product Engineering recommends that the latest firmware level be loaded at system installation.

Minimum firmware levels for MT 8562

The Minimum Ship Level (MSL) firmware for May 2020 shipments is defined as Bundle S20b.

Additional firmware updates were released in Bundle 21 and Bundle S21a, that include important stability and serviceability improvements.

Product Engineering recommends that the latest firmware level be loaded at system installation.

Crypto UDX code considerations

A Crypto UDX (User Defined Extensions) is custom code that is installed in the secure hardware of the Crypto Express card. It allows customers to implement their own unique code within the tamper resistant hardware. On IBM Z, the UDX code is always developed based on customer specifications by IBM (either the Crypto Competence Center in Denmark or IBM Global Services in the United States) and delivered to the customer for installation inside the Crypto card. There is also a key management software package, DKMS, from the Crypto Competence Center that might require a UDX depending, on the customer environment.

Since a UDX interfaces directly with the card and with ICSF (the z/OS component that provides a software interface to the crypto hardware), anytime either a new crypto hardware device is installed or the version of ICSF changes, or specific versions of the crypto code changes, the UDX must be rebuilt. If a customer will be migrating from one hardware device to another (for example, from a Crypto Express5S or Crypto Express6S adapter to a Crypto Express7S in a z15) or upgrading the version of ICSF on their new machine, or migrating to a new driver or MCL with new crypto code, the UDX may need to be rebuilt. The UDX rebuild may delay production workload usage.

In most cases, the contract with the service organization covers rebuilding for new hardware and software platforms. Contact the appropriate organization to have the UDX updated and tested. However, you should allow time in the installation schedule for getting the updated UDXs from IBM. Additionally, if the customer's support contract for the UDX has lapsed, there can be extra time that is required to get the paperwork in place.

Channel information

FICON directors and network switches - minimum levels of code support required for z15 connectivity

IBM Z periodically performs connectivity and interoperability testing of FICON® and FCP switches and directors to ensure that products adhere to the Fibre Connection (FICON) architecture and Fibre Channel Protocol (FCP) architecture.

This information can be found by navigating within the following website:

http://www.ibm.com/servers/resourcelink

1. Click **Sign in**.
2. Specify a valid user ID and password.
3. From the left navigation pane, click **Library**.
4. Locate **Hardware products for servers** heading.
5. Select "Switches and directors qualified for IBM Z FICON and FCP channels" link.

It is important you contact your director and/or switch supplier to determine the minimum level of microcode that is needed when you connect to a z15.

© Copyright IBM Corp. 2019, 2023

Restrictions

See the following restrictions.

Linux Secure Boot restriction with either Bundle S44 or new SLES 15 SP2 or SP3 releases

SUSE recently made an unplanned change to the public key used for Secure Boot/IPL to address a vulnerability (see https://www.suse.com/de-de/support/update/announcement/2021/suse-su-20211238-1/).

- SLES-15-SP2update is described as kernel-default-5.3.18-24.61.1.s390x.rpm, or higher.
- SLES-15-SP3update is described as kernel-default-5.3.18-57.3.s390x.rpm, or higher

Impact

Secure Boot/IPL will fail if there is a mismatch with the platform key and the public key. The net result is that z15 can support only one platform key at a time. This creates a firm co-requisite between z15 and SUSE distribution levels. There are two conditions of concern:

- The new platform key that is contained in Bundle S44 only supports Secure Boot/IPL on the new levels of SUSE. When Bundle S44 is installed, the z15 no longer supports the Secure Boot/IPL on earlier levels of SUSE.
- If the z15 does not have Bundle S44 installed, then customer updates to the newest SUSE distribution, Secure Boot feature will not be supported.

Driver 41C, Bundle S44 can be identified with the installation of MCL022 in the P46640 EC Stream.

Workaround/Actions

- Disable Secure Boot/IPL, on the older levels of SUSE, before installing Bundle S44. Then, perform migrations to the newer SUSE levels before re-enabling Secure Boot.
- Bundle S44 should not be installed, if you are using the Secure Boot capability on an older SUSE distribution.
- Coordinated roll - If you are using Secure Boot, combine the installation of Bundle S44 and update to the newer levels of SUSE distribution.

Linux Secure Boot restriction with Bundle S73a for SLES, RHEL, and Ubuntu

Linux® Secure Boot Restriction with IBM LinuxONE III, IBM LinuxONE III LT2, or IBM z15 D41C Bundle S73a.

D41C Bundle S73a introduces a firmware change that requires a corresponding update to the Linux release/kernel if Linux Secure Boot is to continue to function. Updates are required for SUSE, Red Hat (RHEL), and Canonical (Ubuntu). D41C Bundle S73a was released on May 10, 2023.

The following lists the minimum levels of components for distributions that are required to perform Secure Boot with Linux on Z from FCP-attached disks and NVMe devices on a LinuxONE III, LinuxONE III LT2, or an IBM z15 with D41C Bundle S73a.

Table 1. ***SUSE Linux Enterprise Server:***

Distro	Kernel	s390-tools

© Copyright IBM Corp. 2019, 2023

*Table 1. **SUSE Linux Enterprise Server:** (continued)*		
SLES 15 SP3	kernel-default-5.3.18-150300.59.115.2	s390-tools-2.15.1-150300.8.32.1
SLES 15 SP4	kernel-default-5.14.21-150400.24.55.3	s390-tools-2.19.0-150400.7.18.5

*Table 2. **Red Hat Enterprise Linux:***		
Distro	**Kernel**	**s390utils**
RHEL 8.4	kernel-4.18.0-305.82.1.el8_4	s390utils-2.15.1-5.el8_4.6
RHEL 8.6	kernel-4.18.0-372.46.1.el8_6	s390utils-2.19.0-1.el8_6.3
RHEL 8.7	kernel-4.18.0-425.13.1.el8_7	s390utils-2.22.0-2.el8_7.1
RHEL 9.0	kernel-5.14.0-70.49.1.el9_0	s390utils-2.19.0-2.el9_0.4
RHEL 9.1	kernel-5.14.0-162.22.2.el9_1	s390utils-2.22.0-2.el9_1.1

*Table 3. **Canonical:***		
Distro	**Kernel**	**s390-tools**
Ubuntu 20.04	ubuntu-5.4.0-136.153	2.12.0-0ubuntu3.7
Ubuntu 22.04	ubuntu-5.15.0-57.63	2.20.0-0ubuntu3.2
Ubuntu 22.10	ubuntu-5.19.0-28.29	2.23.0-0ubuntu1.1
Ubuntu 23.04	ubuntu-6.2.0-21.21	2.26.0-0ubuntu1

For SUSE Linux distribution levels

There is a firm Co-Requisite between the IBM zSystems® server or IBM LinuxONE server Bundle level and the SUSE Linux distribution levels in Table 1 on page 13 for Linux Secure Boot to continue to function.

For Red Hat distribution levels

There is a firm Pre-Requisite that those distributions must be updated to the minimum levels shown in Table 2 on page 14 for Linux Secure Boot to continue to function properly when the IBM zSystems server or IBM LinuxONE server Bundle level is updated to D41C Bundle S73a.

For Canonical distribution levels

There is a firm Pre-Requisite that those distributions must be updated to the minimum levels shown in Table 3 on page 14 for Linux Secure Boot to continue to function properly when the IBM zSystems server or IBM LinuxONE server Bundle level is updated to D41C Bundle S73a.

Impact statement

Secure Boot/IPL will fail, if the firm co-requisite or prerequisite between the IBM zSystems server or IBM LinuxONE Bundle level and the Linux distribution levels are not met. The Firmware change can be identified with the installation of MCL P46640.028 in D41C Bundle S73a for LinuxONE III, LinuxONE III LT2, or IBM z15.

Recommended action

If your machine is not using Linux Secure Boot, no further action is needed.

If your machine is using Linux Secure Boot, then consider the following actions.

1. Disable Secure Boot/IPL on the older levels of the Linux distribution, before installing D41C Bundle S73a. Then perform migrations to the newer Linux distribution levels, before re-enabling Secure Boot.

2. Do not install D41C Bundle S73a if you are exploiting the Secure Boot capability on older Linux distributions before the Linux distributions' levels are updated to the minimum levels listed in Table 1 on page 13, Table 2 on page 14, and Table 3 on page 14.
3. Perform a coordinated roll: if you are exploiting Secure Boot, combine the installation of D41C Bundle S73a and the update to the newer levels of the Linux distributions.

Recently removed restrictions

Remote code load for IBM Z

The Early Adopter Program (EAP) has ended and this restriction has been lifted with Driver 41C, Bundles S55 and H37.

Customers that want to use the Remote Code Load feature should contact their local System Service Representative (SSR) if they need assistance when upgrading to Bundles H37 and S55 or higher to enable Remote Code Load support.

CFCC images as a guest under z/VM

Bundle S48 fixed a problem that prevented CFCC images from being IPLed when running as a guest under z/VM®. The origin of this problem was a change made in Bundle S42. The use of native CFCC LPARs was not affected.

Bundle S48 can be identified by the installation of MCL 424 in EC Stream P46598.

Reserved space feature - geographic certifications

All geographic certifications have been completed.

- IBM DS8910F Storage Model 993
- IBM Flash System 7200 or 9200
- IBM Storage Networking SAN32C-6 switches (8977-T32)

Secure Execution for Linux on Z

The Early Adopter Program (EAP) has ended and this is now available to all customers.

The recommended minimum levels are Bundle S39, released on 22 April 2021.

Crypto May 2020 deliveries

The crypto May 2020 deliveries include the following:

- Post Quantum Support for CCA
- Format Preserving Encryption (FPE)
- New ECC Curve support for CCA
- CPACF Extensions

This release requires Bundle S25a, released 24 June 2020.

Bundle S25a can be identified by the activation of MCL 008 in EC Stream P46646.

STP operations - splitting of a CTN network

This release requires Bundle S19 and H11, released 04 March 2020.
Bundle S19 can be identified by the activation of MCL 139 in EC Stream P46598.
Bundle H11 can be identified by the activation of MCL 112 in EC Stream P46683.

© Copyright IBM Corp. 2019, 2023

Standalone dump for SCSI-IPL

z/VM Standalone dump for SCSI first and second level is now available with a PTF for APAR VM66332 and VM66321.
Tested with z15 firmware level Bundle S14, released 15 January 2020.
Bundle S14 can be identified by the activation of MCL 057 in EC Stream P46601.

Crypto deliveries January 2020

Crypto EP11 - protected Key, ECC, and Post Quantum support is now available.
This release requires Bundle S14, released 15 January 2020 along with ICSF APAR OA58358.
Bundle S14 can be identified by the activation of MCL 057 in EC Stream P46601.

Manage power service

Support for managing customer input power maintenance is now available.
This release requires Bundle S13, released 30 December 2019.
Bundle S13 can be identified by the activation of MCL 014 in EC Stream P46610.

Crypto deliveries November 2019

TR-31 function and exploitation of MSA9 for Elliptic Curve Cryptography(ECC) in CCA mode.
This release requires Bundle S07, released 18 October 2019 along with ICSF APAR OA58377.
Bundle S07 can be identified by the activation of MCL 004 in EC Stream P46646.

Dynamic operations on SACF (standalone coupling facility)

This release requires Bundle S20, released 08 April 2020.
Bundle S19 can be identified by the activation of MCL 173 in EC Stream P46598.

Software Secure Service Container appliance images

Software Secure Service Container (SSC) appliance images are not currently supported. This includes IZOA (that is, zAware), VIDAA and Hyper Protect, SSC4ICP.

This restriction is removed with a combination of items:

- Installation of Bundle S10, released to zRSF on 25 November 2019
- Connections to zRSF, where records will be refreshed from IBM Resource Link

z/VM standalone dump

z/VM standalone dump requires PFTs for APARs VM66321 and VM66322.

Exceptions

Problem

PCI-HSM certification of CCA 7.4.*(7S) and CCA 6.7.*(6S) is pending. These levels were released on 25 August 2021 in Bundle S48a.

Crypto Express7S - 7.4.* level can be identified with MCL016 in EC Steam P46646.
Crypto Express6S - 6.7.* level can be identified with MCL011 in EC Steam P46644.

Impact

This can affect PCI PIN audited workloads that rely on the PCI-HSM certification. Refer to PCI Security Standards website for the latest approved levels.

Crypto Express7S at https://www.pcisecuritystandards.org/popups/pts_device.php?appnum=4-20358
Crypto Express6S at https://www.pcisecuritystandards.org/popups/pts_device.php?appnum=4-20358

Workaround

If PCI-HSM certification is required, contact next-level-support for assistance regarding the installation of Bundles S48a or higher.

Problem

PCI-HSM, might report generated DES tokens as non-compliant due to Bundle S39a Crypto CCA change that enforces the new PCI-HSM compliance mode. This affects both Crypto Express 6S and Crypto Express7S features.

Impact

With the Bundle S39a, released 5 May 2021, new compliant-tag DES tokens will have a X’03’ at offset 15 as the KDF value. Compliant-tagged tokens from earlier releases with X'01' or X'02' at offset 15 are no longer considered compliant and might not function in some services.

Workaround

DES compliant-tagged X'01' or X'02'-KDF tokens should be migrated according to instructions in APAR OA60318 for ICSF FMID HCR77D1. This APAR was released on 6 May 2021. Refer to APAR documentation for details.

Problem

Crypto EP11 TKE Configuration Migration from z14 with Bundle S41a without S43a.

Impact

The file that was exported from the z14 might be corrupted or unusable.

Workaround

Ensure the z14 has installed MCL 006 in EC Stream P41459, then perform the migration again.

This fix was made available 30 September 2020 as part of Bundle S43a.

Problem

PDU LED colors are not consistent across all systems or configurations.

PDU LED colors can be green or amber, or they can change from amber to green. Root cause ties to the internal PDU build levels.

Action

Does not affect repair actions. R&V does not rely upon the color of the LEDs.

Problem

Power® consumption values that are shown on the Monitors Dashboard might not be correct.

Action

See the *Installation Manual for Physical Planning* for estimated power values until a firmware solution is available.

© Copyright IBM Corp. 2019, 2023

Problem

For T02 models (MT 8562), fan speed settings and power consumption might be higher than what is specified in the *Installation Manual for Physical Planning*.

Action

Firmware updates will soon be released to correct this issue.

Problem

Recoverable channel control checks can be reported to the operating systems.

Action

No action is required unless errors are persistent. Report a problem to IBM.

Problem

At installation time, refcode E0610061 0000B00B can be reported if Bundle S21 is not installed.

This is a VPD build error, when PDUs are used in a single phase operation. Power system is fully operational.

Action

Install Bundle S21, then perform the **Rebuild VPD and HOM** task.

Problem

Activate (IML) and/or Power off/Deactivate might fail with various errors.

Action

Retry operation. If it is not successful, contact next level support.

Problem

FICON can surface channel control checks.

Details

Recoverable errors can be reported to the operating system.

Action

No action is required unless errors are persistent. Report a problem to IBM.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on http://www.ibm.com/trademark.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

© Copyright IBM Corp. 2019, 2023

SC28-7001-00