

CA Top Secret Security for z/OS 15.0  
CA RS 1503 Service List

Release	Service	Description	Type
15.0	RO74485	BUILD UP OF SP229 KEY 8 IN CICS AFTER TSS REFRESH	PTF
	RO75325	MISSING RESOURCE CLASS / NAME ON OBJECT ACCESS EVENTS	PTF
	RO76973	PERMIT W/ACC(NONE) INCORRECTLY SELECTED AFTER RO68148	*HIP/PRP*
	RO77239	ABEND S002 IN TSSCIALD DURING CIA UNLOAD	PTF
	RO77322	MULTIPLE TSSC056W MESSAGES WHEN ACID PERMIT SENT TO CIART	PTF
	RO78265	LOADING CAS4MSG RETURNS BAD EP ADDRESS AFTER TSS IS RECYCLED	*HIP/PRP*
	RO78283	UTIL RPT-DRC      GARBAGE	PTF
	RO78786	COMPARE CMD BAD OUTPUT CESS=	PTF
	RO78876	SMSBCKUP,VSAMDEF1&2 UPDATE	PTF

The CA RS 1503 service count for this release is 9

CA Top Secret Security for z/OS  
CA RS 1503 Service List for CAKOF00

FMID	Service	Description	Type
CAKOF00	RO74485	BUILD UP OF SP229 KEY 8 IN CICS AFTER TSS REFRESH	PTF
	RO75325	MISSING RESOURCE CLASS / NAME ON OBJECT ACCESS EVENTS	PTF
	RO76973	PERMIT W/ACC(NONE) INCORRECTLY SELECTED AFTER RO68148	*HIP/PRP*
	RO77239	ABEND S002 IN TSSCIALD DURING CIA UNLOAD	PTF
	RO77322	MULTIPLE TSSC056W MESSAGES WHEN ACID PERMIT SENT TO CIART	PTF
	RO78265	LOADING CAS4MSG RETURNS BAD EP ADDRESS AFTER TSS IS RECYCLED	*HIP/PRP*
	RO78283	UTIL RPT-DRC      GARBAGE	PTF
	RO78786	COMPARE CMD BAD OUTPUT CESS=	PTF
	RO78876	SMSBCKUP,VSAMDEF1&2 UPDATE	PTF

The CA RS 1503 service count for this FMID is 9

CA Top Secret Security for z/OS 15.0  
CA RS 1503 - PTF RO74485 Details

Release	Service	Details
15.0	RO74485	<p>RO74485 M.C.S. ENTRIES = ++PTF (RO74485)</p> <p>BUILD UP OF SP229 KEY 8 IN CICS AFTER TSS REFRESH</p> <p>PROBLEM DESCRIPTION: Deadmain of storage in subpool 229 key 8 in the CICS region address space can lead to a failure of the region. This problem shows up when OPTIONS(38) is set and a TSS REFRESH command is issued on an acid that has logged on via CICS VERIFY signon.</p> <p>SYMPTOMS: Private storage in the CICS address space subpool 229 key 8 grows first above the line, then below until the region runs out of storage. The following messages were reported when the problem occurred.</p> <p>+DFHMN0001 CICS99W An abend (code 653/AKEB) has occurred at offset X'FFFF' in module DFHMNSU. +DFHME0116 CICS99W 792 (Module:DFHMEME) CICS symptom string for message DFHMN0001 is PIDS/5655S9700 LVLS/670 MS/DFHMN0001 RIDS/DFHMNSU PTFS/HCI6700 AB/S0653 AB/UAKEB ADRS/0000FFFF</p> <p>IMPACT: Once all of the storage is exhausted, the CICS region either terminates or goes into an ABEND loop. This can affect all CICS releases.</p> <p>CIRCUMVENTION: Do not issue TSS REFRESH command against an ACID if logged on via attachsec verify in CICS.</p> <p>PRODUCT(S) AFFECTED: CA Top Secret for z/OS <span style="float: right;">Release 15.0</span> Release 14.0 Star Problem(s): TSSMVS 9601 Copyright (C) 2015 CA. All rights reserved. R01035-TSS150-SP1</p> <p>DESC(BUILD UP OF SP229 KEY 8 IN CICS AFTER TSS REFRESH). ++VER (Z038) FMID (CAKOF00) PRE ( RO25900 RO55678 ) SUP ( TR51086 TR51141 TR51145 RO51145 TR74485 TR78626 ) ++HOLD (RO74485) SYSTEM FMID(CAKOF00) REASON (DYNACT ) DATE (15054) COMMENT (</p> <pre> +-----+        CA Top Secret for z/OS                      Release 15.0        +-----+  SEQUENCE   After Apply  +-----+  PURPOSE    Correct Buildup of Subpool 229 key 8 after refresh                ACID in CICS using ATTACHSEC Verify                  +-----+  USERS      All users that issue Refresh ACEE in CICS using      AFFECTED   Attachsec Verify                                      +-----+  KNOWLEDGE  1- Product Administration                             REQUIRED   2- SMP/e  3- CICS Systems Programming                                      4- Security Administration                           +-----+  ACCESS     SMP/e CSI libraries                                   REQUIRED  +-----+ ***** * STEPS   TO   PERFORM * ***** LLA,REFRESH Recycle of TSS with REINT ).</pre>

CA Top Secret Security for z/OS 15.0  
CA RS 1503 - PTF RO75325 Details

Release	Service	Details
15.0	RO75325	<p>RO75325 M.C.S. ENTRIES = ++PTF (RO75325)</p> <p>MISSING RESOURCE CLASS / NAME ON OBJECT ACCESS EVENTS PROBLEM DESCRIPTION: Compliance Manager object access event records may contain an empty object class column and/or an empty object entity column when the type of event being recorded is a RACROUTE EXTRACT request. SYMPTOMS: When viewing the object access event records you will see events where the object class column is blank/null, the object entity column is blank/null, or both columns are blank/null. IMPACT: Compliance manager reporting will contain event records that reflect object access events that have no meaning when they do not contain the appropriate columns of data. CIRCUMVENTION: None available. PRODUCT(S) AFFECTED: CA Top Secret for z/OS <span style="float: right;">Release 15.0</span> Star Problem(s): TSSMVS 9588 Copyright (C) 2014 CA. All rights reserved. R01049-TSS150-SP1</p> <p>DESC(MISSING RESOURCE CLASS / NAME ON OBJECT ACCESS EVENTS). ++VER (Z038) FMID (CAKOF00) PRE ( RO26450 RO47730 RO55678 ) SUP ( RO24344 RO25077 RO27279 RO41076 RO48059 RO53077 RO54379 RO55069 RO63094 RO64045 RO67706 TR24211 TR24344 TR25077 TR27279 TR41076 TR44357 TR48059 TR53077 TR54379 TR54504 TR55069 TR63094 TR63379 TR64045 TR67706 TR71948 TR75325 ) ++HOLD (RO75325) SYSTEM FMID(CAKOF00) REASON (DYNACT ) DATE (14328) COMMENT (</p> <pre> +-----+            CA Top Secret for z/OS                      Release 15.0            +-----+-----+  SEQUENCE   After Apply  +-----+-----+  PURPOSE    Load module into LLA and activate                      +-----+-----+  USERS      All   AFFECTED  +-----+-----+  KNOWLEDGE  1. Console commands                                     REQUIRED   2. Top Secret administration                            +-----+-----+  ACCESS     1. Console authority                                     REQUIRED   2. TSS administrative authority                         +-----+-----+ ***** * STEPS TO PERFORM * ***** SMP APPLY, LLA REFRESH and restart CA Top Secret with TSS,,REINIT ). </pre>

CA Top Secret Security for z/OS 15.0  
CA RS 1503 - PTF RO76973 Details

Release	Service	Details
15.0	RO76973	<p>RO76973 M.C.S. ENTRIES = ++PTF (RO76973)</p> <p>PERMIT W/ACC(NONE) INCORRECTLY SELECTED AFTER RO68148</p> <p>PROBLEM DESCRIPTION: After CA Top Secret RO68148 is implemented, the following problem can occur. A TSS PERMIT with ACC(NONE) is incorrectly selected by the security algorithm for maskable RIE resources.</p> <p>SYMPTOMS: A less restrictive permit may be selected if it has ACCESS(NONE) resulting in violations that should not occur.</p> <p>IMPACT: Users receive violations for resource entities they should be allowed to access.</p> <p>CIRCUMVENTION: None.</p> <p>PRODUCT(S) AFFECTED: CA Top Secret for z/OS <span style="float: right;">Release 15.0</span></p> <p>Star Problem(s): TSSMVS 9634</p> <p>Copyright (C) 2014 CA. All rights reserved. R01068-TSS150-SP1</p> <p>DESC(PERMIT W/ACC(NONE) INCORRECTLY SELECTED AFTER RO68148). ++VER (Z038) FMID (CAKOF00) PRE ( RO25204 ) SUP ( AR68148 RO25214 RO25960 RO40757 RO61772 RO68148 TR24258 TR25214 TR25960 TR40757 TR61772 TR68148 TR76837 TR76973 ) ++HOLD (RO76973) SYSTEM FMID(CAKOF00) REASON (DYNACT ) DATE (14365) COMMENT (</p> <pre> +-----+        CA Top Secret for z/OS                      Release 15.0        +-----+  SEQUENCE   After Apply                                       +-----+  PURPOSE    Install maintenance.                               +-----+  USERS      Users who applied apar RO68148.                    AFFECTED  +-----+  KNOWLEDGE  1- SMP/e  REQUIRED   2- z/OS Systems Programming                                    3- z/OS Operator Commands                         +-----+  ACCESS     SMP/e CSI libraries                                REQUIRED  +-----+ ***** * STEPS   TO   PERFORM * ***** SMP APPLY, LLA REFRESH and restart CA Top Secret ).</pre>

CA Top Secret Security for z/OS 15.0  
 CA RS 1503 - PTF RO77239 Details

Release	Service	Details
15.0	RO77239	<p>RO77239 M.C.S. ENTRIES = ++PTF (RO77239)</p> <p>ABEND S002 IN TSSCIALD DURING CIA UNLOAD            PROBLEM DESCRIPTION:            Abend S002 with RC=18 can occur in module TSSCIALD during the batch CIA unload process.            SYMPTOMS:            IEC036I 002-18,IGC0005E,J03120SA,CIAUNLD,UNLOAD,E802,PRMT11,CAI.CHRSEC40.CIA0400.UNLOAD            IMPACT:            The batch load abends and cannot be complete successfully.            CIRCUMVENTION:            None.            PRODUCT(S) AFFECTED:            CA Top Secret for z/OS <span style="float: right;">Release 15.0</span>            Star Problem(s):            TSSMVS 9627            Copyright (C) 2015 CA. All rights reserved. R01073-TSS150-SP1</p> <p>DESC(ABEND S002 IN TSSCIALD DURING CIA UNLOAD).            ++VER (Z038)            FMID (CAKOF00)            PRE ( RO35644 RO36198 RO36912 RO47730 RO50925 RO55372            RO77159 )            SUP ( TR42348 RO42348 TR51709 TR54274 TR61173 TR61185            TR64901 TR63858 TR66458 RO64901 TR70640 RO66458 RO70640            TR76157 TR77239 )            ++HOLD (RO77239) SYSTEM FMID(CAKOF00)            REASON (DYNACT ) DATE (15026)            COMMENT (</p> <pre> +-----+            CA Top Secret for z/OS                      Release 15.0            +-----+  SEQUENCE   After Apply   +-----+  PURPOSE    Activate maintenance without an IPL                      +-----+  USERS      All users   AFFECTED   +-----+  KNOWLEDGE  SMP/E   REQUIRED   z/OS Systems programming  Product installation                                    +-----+  ACCESS     SMP/E CSI libraries                                       REQUIRED   +-----+ ***** * STEPS    TO    PERFORM * ***** 1. SMP APPLY 2. LLA REFRESH 3. Shutdown and restart CIA real time (CIARTUPD) address space ). </pre>

CA Top Secret Security for z/OS 15.0  
 CA RS 1503 - PTF RO77322 Details

Release	Service	Details
15.0	RO77322	<p>RO77322 M.C.S. ENTRIES = ++PTF (RO77322)</p> <p>MULTIPLE TSSC056W MESSAGES WHEN ACID PERMIT SENT TO CIART            PROBLEM DESCRIPTION:            CIA Realtime incorrectly handles cross authorization ACID permits.            SYMPTOMS:            Message TSSC056W issued for XAUTH ACID permits.            IMPACT:            CIA database may get out of sync with TSS security file.            CIRCUMVENTION:            None.            PRODUCT(S) AFFECTED:            CA Top Secret for z/OS <span style="float: right;">Release 15.0</span>            Star Problem(s):            TSSMVS 9625            Copyright (C) 2015 CA. All rights reserved. R01074-TSS150-SP1</p> <p>DESC(MULTIPLE TSSC056W MESSAGES WHEN ACID PERMIT SENT TO CIART).            ++VER (Z038)            FMID (CAKOF00)            PRE ( RO36198 RO36912 RO47730 RO50925 RO58844 RO77159 )            SUP ( RO73213 TR73213 TR74435 TR76773 TR77322 )            ++HOLD (RO77322) SYSTEM FMID(CAKOF00)            REASON (DYNACT ) DATE (15055)            COMMENT (</p> <pre> +-----+            CA Top Secret for z/OS                     Release 15.0            +-----+  SEQUENCE   After Apply                               +-----+  PURPOSE    Install maintenance.                       +-----+  USERS      Users that implement CIA Real Time.         AFFECTED   +-----+  KNOWLEDGE  1- SMP/e                                    REQUIRED   2- z/OS Systems Programming                             3- z/OS Operator Commands                              +-----+  ACCESS     SMP/e CSI libraries                         REQUIRED   +-----+ ***** * STEPS TO PERFORM * ***** SMP APPLY, LLA REFRESH and restart CIA RealTime STC. ).</pre>

CA Top Secret Security for z/OS 15.0  
CA RS 1503 - PTF RO78265 Details

Release	Service	Details
15.0	RO78265	<p>RO78265 M.C.S. ENTRIES = ++PTF (RO78265)</p> <p>LOADING CAS4MSG RETURNS BAD EP ADDRESS AFTER TSS IS RECYCLED PROBLEM DESCRIPTION: When PDSPROT is enabled after TSS is recycled, a bad entry point address may be returned when CAS4INIT loads module CAS4MSG. SYMPTOMS: TSS9681A CA-TSS SECURITY FILE SERVICES ABEND S0C4 IN TSSMNGR+37762 and possibly additional abends. IMPACT: A system IPL is required. CIRCUMVENTION: Do not enable PDSPROT after TSS is recycled. PRODUCT(S) AFFECTED: CA Top Secret for z/OS <span style="float: right;">Release 15.0</span> Star Problem(s): TSSMVS 9649 Copyright (C) 2015 CA. All rights reserved. R01085-TSS150-SP1</p> <p>DESC(LOADING CAS4MSG RETURNS BAD EP ADDRESS AFTER TSS IS RECYCLED). ++VER (Z038) FMID (CAKOF00) PRE ( RO24069 RO25587 RO26450 RO36198 RO37109 RO38472 RO45811 RO50143 RO50925 RO55678 RO60611 RO63150 RO63740 RO66142 RO68239 RO68259 RO70449 ) SUP ( CC56243 DC56243 LC56243 RI63057 RO40589 RO42155 RO42988 RO58021 RO58318 RO63014 RO65810 RO77812 TR16265 TR16732 TR31112 TR31438 TR40589 TR42155 TR42988 TR57058 TR57652 TR58021 TR58318 TR60294 TR63014 TR65810 TR77812 TR78265 ) ++HOLD (RO78265) SYSTEM FMID(CAKOF00) REASON (DYNACT ) DATE (15057) COMMENT (</p> <pre> +-----+            CA Top Secret for z/OS                     Release 15.0            +-----+-----+  SEQUENCE   After Apply   +-----+-----+  PURPOSE    Install maintenance.   +-----+-----+  USERS      users that implement PDS/Member protection.    AFFECTED   +-----+-----+  KNOWLEDGE   1- SMP/e    REQUIRED    2- z/OS Systems Programming                3- z/OS Operator Commands                +-----+-----+  ACCESS     SMP/e CSI libraries    REQUIRED   +-----+-----+ ***** * STEPS TO PERFORM * ***** SMP APPLY, LLA REFRESH and restart CA Top Secret ). </pre>

CA Top Secret Security for z/OS 15.0  
 CA RS 1503 - PTF RO78283 Details

Release	Service	Details
15.0	RO78283	<pre> RO78283  M.C.S. ENTRIES  = ++PTF (RO78283)  UTIL RPT-DRC      GARBAGE PROBLEM DESCRIPTION: TSSUTIL produces garbage in the last 4 characters of the entity name in the TSSUTIL LONG report for TSOACCT resources. The problem seems to occur when 'TRAPS NAME(IGVINITGETMAIN,IGVINITFREEMAIN)' is used in SYS1.PARMLIB(DIAGxx) SYMPTOMS: The sample event looked like: DATE      TIME      SYSID ACCESSOR  JOBNAME  FACILITY  MODE 01/28/15  15:36:17  XE56  UTACCT    UTACCT    TSO      FAIL RESOURCE  TYPE &amp; NAME :   TSOACCT  11820000 VC  PROGRAM  R-ACCESS A-ACCESS SRC/DRC  SEC  JOBID  TERMINAL IKJEFLC                                OK+A                                A55TU005      IMPACT: None CIRCUMVENTION: Do not set SYS1.PARMLIB(DIAGxx) with 'TRAPS NAME(IGVINITGETMAIN,IGVINITFREEMAIN)' PRODUCT(S) AFFECTED: CA Top Secret for z/OS                                     Release 15.0 Star Problem(s): TSSMVS 9647 Copyright (C) 2015 CA. All rights reserved. R01086-TSS150-SP1  DESC(UTIL RPT-DRC      GARBAGE). ++VER (Z038) FMID (CAKOF00) PRE ( R018634 R019256 R035644 R036198 R067185 ) SUP ( TR31217 R031217 TR55095 TR56352 TR64641 R064641 TR78283 ) ++HOLD (RO78283) SYSTEM FMID(CAKOF00) REASON (DYNACT )   DATE (15042) COMMENT ( +-----+            CA Top Secret for z/OS                      Release 15.0            +-----+  SEQUENCE   After Apply   +-----+  PURPOSE    Load modules into memory and activate                   +-----+  USERS      TSS Auditors  AFFECTED   +-----+  KNOWLEDGE  1. Console commands  REQUIRED   2. Top Secret administration                               +-----+  ACCESS     1. Console authority  REQUIRED   2. TSS administrative authority                             +-----+ ***** * STEPS   TO   PERFORM * ***** SMP APPLY, LLA REFRESH and a restart of TSS is required to install this APAR. ).</pre>

Release	Service	Details
15.0	RO78786	<p>RO78786 M.C.S. ENTRIES = ++PTF (RO78786)</p> <p>COMPARE CMD BAD OUTPUT CESS=            PROBLEM DESCRIPTION:            The output of the TSS COMPARE(acid1) USING(acid2) command, where one of the ACIDs has a permit in the CPCMD or DIAGNOSE resource class, shows garbage characters "..CESS".            SYMPTOMS:            When comparing two ACIDs, "..CESS=" is incorrectly added to the output of one IMPACT:            Cosmetic; The "..CESS=" does not overlay any of the other output in the 'Permit Differences' section for CPCMD or DIAGNOSE resource class            PRODUCT(S) AFFECTED:            CA Top Secret for z/OS <span style="float: right;">Release 15.0</span>            Star Problem(s):            TSSMVS 9655            Copyright (C) 2015 CA. All rights reserved. R01096-TSS150-SP1</p> <p>DESC(COMPARE CMD BAD OUTPUT CESS=).            ++VER (Z038)            FMID (CAKOF00)            PRE ( RO55678 )            SUP ( BC56243 ER55678 RO20765 RO21040 RO21789 RO57893            RO61247 TR16986 TR17334 TR17629 TR17994 TR20229            TR20765 TR21040 TR21616 TR21789 TR57893 TR61247            TR78786 )            ++HOLD (RO78786) SYSTEM FMID(CAKOF00)            REASON (DYNACT ) DATE (15055)            COMMENT (            +-----+              CA Top Secret for z/OS <span style="float: right;">Release 15.0</span>              +-----+             SEQUENCE   After Apply              +-----+             PURPOSE   Load module into LLA and activate              +-----+             USERS   All               AFFECTED                +-----+             KNOWLEDGE   1. Console commands               REQUIRED   2. Top Secret administration              +-----+             ACCESS   1. Console authority               REQUIRED   2. TSS administrative authority              +-----+            *****            * STEPS TO PERFORM *            *****            SMP APPLY, LLA REFRESH and restart CA Top Secret            ).</p>

Release	Service	Details
15.0	RO78876	<p>RO78876 M.C.S. ENTRIES = ++PTF (RO78876)</p> <p>SMSBCKUP &amp; VSAMDEF1 MEMBERS</p> <p>PROBLEM DESCRIPTION:            Update to members SMSBCKUP, VSAMDEF1, and VSAMDEF2 in the TSS r15 CAKOJCL0 library</p> <p>SYMPTOMS:            N/A</p> <p>IMPACT:            N/A</p> <p>CIRCUMVENTION:            N/A</p> <p>PRODUCT(S) AFFECTED:            CA Top Secret for z/OS <span style="float: right;">Release 15.0</span>            Star Problem(s):            TSSMVS 9644</p> <p>Copyright (C) 2015 CA. All rights reserved. R01100-TSS150-SP1</p> <p>DESC(SMSBCKUP,VSAMDEF1&amp;2 UPDATE).            ++VER (Z038)            FMID (CAKOF00)            SUP ( TR78876 )            ++HOLD (RO78876) SYSTEM FMID(CAKOF00)            REASON (DYNACT ) DATE (15056)            COMMENT (</p> <pre> +-----+            CA Top Secret for z/OS                     Release 15.0            +-----+  SEQUENCE   After Apply                               +-----+  PURPOSE    Load module into LLA and activate          +-----+  USERS      ALL  AFFECTED   +-----+  KNOWLEDGE  1. Console commands                          REQUIRED   2. Top Secret administration               +-----+  ACCESS     1. Console authority                        REQUIRED   2. TSS administrative authority            +-----+ ***** * STEPS TO PERFORM * ***** SMP APPLY ).</pre>