Release	Service	Description	Hiper
15.0	RO64546	ABEND S0C4 IN CAKSMSGH, EMPTY BUFFER	
	RO65762	CAS9578E ABEND REGION OUT OF STORAGE BELOW THE LINE	
	RO66142	ALLOW TSS SPOOL FILES TO BE CLOSED DYNAMICALLY	
	RO67185	SUPPORT Z/OS CHANGES IN PKI SERVICES	
	RO68057	SIGNALG VALID ONLY ON GENCERT	
	RO68239	SUPPORT MIRRORED SECURITY FILE	
	RO68361	AUTOUID IMPROPERLY SENT TO PASSWORD-ONLY NODES	**HIPER**
	RO68393	AT TIMES THE DFLTGRP NOT ADDED TO THE GROUP LIST	**HIPER**
	RO68435	ABEND S0C4 IN TSSAUTHA ON REFRESH JOBNAME(*)	
	RO68831	TSSAUDIT RETURN CODE PROCESSING	
	RO69065	OVERLAY OF CSA WITH PKISERV AND OPTION(32) ACTIVE	**HIPER**
The CA RS 1405 service count for this release is 11			

Release	Service	Description	Hiper
14.0	NO-SRVC	CA RS 1405 Contains No Service For This Release of This Product.	
The CA RS 1405 service count for this release is 0			

FMID	Service	Description	Hiper
CAKOF00	RO65762	CAS9578E ABEND REGION OUT OF STORAGE BELOW THE LINE	
	RO66142	ALLOW TSS SPOOL FILES TO BE CLOSED DYNAMICALLY	
	RO67185	SUPPORT Z/OS CHANGES IN PKI SERVICES	
	RO68057	SIGNALG VALID ONLY ON GENCERT	
	RO68239	SUPPORT MIRRORED SECURITY FILE	
	RO68361	AUTOUID IMPROPERLY SENT TO PASSWORD-ONLY NODES	**HIPER**
	RO68393	AT TIMES THE DFLTGRP NOT ADDED TO THE GROUP LIST	**HIPER**
	RO68435	ABEND S0C4 IN TSSAUTHA ON REFRESH JOBNAME(*)	
	RO68831	TSSAUDIT RETURN CODE PROCESSING	
	RO69065	OVERLAY OF CSA WITH PKISERV AND OPTION(32) ACTIVE	**HIPER**
The CA RS 1405 service count for this FMID is 10			

FMID	Service	Description	Hiper
CAKOF01	RO64546	ABEND S0C4 IN CAKSMSGH, EMPTY BUFFER	
The CA RS 1405 service count for this FMID is 1			

Release	Service	Details
15.0	RO64546	RO64546 M.C.S. ENTRIES = ++PTF (RO64546) ABEND S0C4 IN CAKSMSGH, EMPTY BUFFER PROBLEM DESCRIPTION: An invalid (binary zero) message buffer causes CAKSMSGH to ABEND with a S0C4 while processing. The zero buffer was caused when an 'EXEC CICS START TRANID' was issued just before the link to TSSCICS. The code has been updated to handle this situation and also issue a TAZ5 ABEND if an invalid buffer is detected. SYMPTOMS: A CICS transaction dump is taken and the transaction fails. The CICS region continues to process. IMPACT: TSS transaction fails. CIRCUMVENTION: Try to reissue the TSS transaction. If that does not work try to issue the transaction in TSO. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 CA Top Secret for z/OS Release 14.0 Star Problem(s): TSSMVS 9506 Copyright (C) 2014 CA. All rights reserved. R00883-TSS150-SP1 DESC(ABEND S0C4 IN CAKSMSGH, EMPTY BUFFER) . ++VER (Z038) FMID (CAKOF01) PRE (RO26389 RO32608 RO35678 RO43979 RO53625 RO64897) SUP (TR25733 AR35678 RO25733 TR31788 TR38667 RO38667 TR46000 TR46119 RO46119 TR50439 AR50439 TR53765 RO50439 RO53765 RO40965 TR40381 TR40592 TR40965 TR64546) ++HOLD (RO64546) SYSTEM FMID(CAKOF01) REASON (ACTION) DATE (14079) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Issue a TAZ5 abend when a invalid buffer is pass | | | to CAKSMSGH to process for diagnostic | +----------+----------+ |USERS | | |AFFECTED | All users leveraging CICS interface. | +----------+----------+ +----------+----------+ |KNOWLEDGE | 1 - 1- Product Administration | |REQUIRED | 2 - SMP/E | | | 3 - z/OS Systems Programming | | | 4 - Security Administration | +----------+----------+ |ACCESS | SMP/E CSI Libraries | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** 1. LLA Refresh 2. Recycle the CICS region).

Release	Service	Details
15.0	RO65762	RO65762 M.C.S. ENTRIES = ++PTF (RO65762) CAS9578E ABEND REGION OUT OF STORAGE BELOW THE LINE PROBLEM DESCRIPTION: CICS ABENDS during a security check when the region runs out of below the line storage. The region will likely abend because of the short on storage condition. CA Top Secret is a victim of this out of storage condition. CA Top Secret needs to return to the caller to handle the storage shortage problem. SYMPTOMS: CAS9578E - PRODUCT = KO50 PSW = 070C2000 C780C8E0 COMPLETION CODE = 00C1 IMPACT: The job abends. CIRCUMVENTION: Determine who is allocating the storage below the line (24) and correct as needed. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9526 Copyright (C) 2013 CA. All rights reserved. R00907-TSS150-SP1 DESC(CAS9578E ABEND REGION OUT OF STORAGE BELOW THE LINE) . ++VER (Z038) FMID (CAKOF00) PRE (RO18784 RO19158 RO25587 RO32654 RO35644 RO36198 RO45458 RO46592 RO47831 RO47860 RO55678 RO58366 RO63740) SUP (TR26491 RO26491 TR27036 RO27036 TR36860 TR41888 TR42119 TR43837 RO36860 RO43837 TR50077 AR45458 AR50077 RO50077 TR53696 TR53985 TR54009 RO53985 TR55023 RO55023 TR59666 IR55678 RO59666 TR64729 RO64729 TR65762) ++HOLD (RO65762) SYSTEM FMID(CAKOF00) REASON (ACTION) DATE (13351) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Return to caller when storage is exhausted below the line.| +----------+----------+ |USERS | Application issuing branch enter security request. | |AFFECTED | | +----------+----------+ |KNOWLEDGE | 1 - 1- Product Administration | |REQUIRED | 2 - SMP/E | | | 3 - z/OS Systems Programming | | | 4 - Security Administration | +----------+----------+ |ACCESS | SMP/E CSI Libraries | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** 1. LLA Refresh 2. Recycle the TSS,,,REINIT).

Release	Service	Details
15.0	RO66142	RO66142 M.C.S. ENTRIES = ++PTF (RO66142) ALLOW TSS SPOOL FILES TO BE CLOSED DYNAMICALLY PROBLEM DESCRIPTION: Introduce the new SYSOUT(CLOSE) Control Option setting for JES3 clients only. This option will close all currently open Top Secret spool files including the journal files for CPF and LDAP and the $$$LOG$$ file. This option is only valid if CA Top Secret is running SUB=MSTR and JES3 is active. If this option is entered while TSS is running under JES3 or while JES2 is active you will see the following messages: TSS9079E INVALID DATA TSS9076I CURRENT OPTION IS <CLOSE> TSS9078I MODIFY OPTION IGNORED SYSOUT(CLOSE) is for use at system shutdown. The only way to get the spool files back is a restart of CA Top Secret PRIOR to shutting down JES3. Once JES3 has been shut these cannot be reopened and CA Top Secret cannot be restarted. SYMPTOMS: None. IMPACT: This enhancement is provided to allow JES3 sites to properly shut down JES3 global nodes while the TSS started task is still active. CIRCUMVENTION: If SUB=MSTR is required for JES3 sites then TSS must be stopped prior to shutting down the JES3 global node. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9525 Copyright (C) 2013 CA. All rights reserved. R00919-TSS150-SP1 DESC(ALLOW TSS SPOOL FILES TO BE CLOSED DYNAMICALLY) . ++VER (Z038) FMID (CAKOF00) PRE (RO18784 RO25587 RO26450 RO32653 RO35644 RO36198 RO37109 RO38472 RO43262 RO45811 RO47730 RO48248 RO48562 RO50925 RO55678 RO60611 RO63150 RO63740) SUP (TR21478 TR17457 TR36616 TR37235 TR16265 TR16732 TR40589 TR42155 TR42988 TR46685 TR48278 TR47373 TR48614 TR48724 RO40589 RO42155 RO42988 RO48278 RO48724 TR50143 TR55513 TR31112 TR31438 TR57058 TR57652 TR58021 RO58021 TR58318 TR59441 CC56243 DC56243 RI63057 RO58318 TR60294 TR63014 RO21478 RO37235 RO50143 RO55513 RO59441 RO63014 TR31827 TR65773 TR66142) ++HOLD (RO66142) SYSTEM FMID(CAKOF00) REASON (DYNACT) DATE (13354) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Load module into LLA allow use of new control option | +----------+----------+ |USERS | All JES3 clients | |AFFECTED | | +----------+----------+ |KNOWLEDGE | 1. Console commands | |REQUIRED | 2. Top Secret administration | +----------+----------+ |ACCESS | 1. Console authority | |REQUIRED | 2. TSS administrative authority | +----------+----------+ ********** * STEPS TO PERFORM * **********

Release	Service	Details
		SMP APPLY, LLA REFRESH and restart CA Top Secret).

Release	Service	Details
15.0	RO67185	RO67185 M.C.S. ENTRIES = ++PTF (RO67185) SUPPORT Z/OS CHANGES IN PKI SERVICES PROBLEM DESCRIPTION: Support for z/OS 2.1 changes in PKI Services SYMPTOMS: Inability to create/modify/remove certificates in PKI Services on z/OS 2.1 IMPACT: PKI Services may not be usable on z/OS 2.1 CIRCUMVENTION: N/A PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9548 Copyright (C) 2014 CA. All rights reserved. R00937-TSS150-SP1 DESC(SUPPORT Z/OS CHANGES IN PKI SERVICES) . ++VER (Z038) FMID (CAKOF00) PRE (RO18634 RO19256 RO20174 RO25900 RO35644 RO36198 RO55678) SUP (AR64969 RO26597 RO31217 RO64641 RO64969 RO66128 TR24965 TR25529 TR26597 TR31217 TR55095 TR56352 TR64641 TR64969 TR66128 TR67185) ++HOLD (RO67185) SYSTEM FMID(CAKOF00) REASON (DYNACT) DATE (14119) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Support z/OS 2.1 PKI Services | +----------+----------+ |USERS | All users that use PKI Services to manage digital | |AFFECTED | certificates | +----------+----------+ |KNOWLEDGE | 1 - SMP/E | |REQUIRED | 2 - z/OS Systems Programming | | | 3 - Security Administration | +----------+----------+ |ACCESS | SMP/E CSI Libraries | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** 1. LLA Refresh 2. Refresh SAF using F TSS,REFRESH(SAF) 3. Recycle using TSS,,,REINIT).

Release	Service	Details
15.0	RO68057	RO68057 M.C.S. ENTRIES = ++PTF (RO68057) SIGNALG VALID ONLY ON GENCERT PROBLEM DESCRIPTION: SIGNALG parm is only valid for a CA Top Secret GENCERT command. SYMPTOMS: Command just ignores parm, without any indication that SIGNALG is not being used. IMPACT: No error message received. CIRCUMVENTION: Remove SIGNALG from the GENCERT command. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9496 Copyright (C) 2014 CA. All rights reserved. R00949-TSS150-SP1 DESC(SIGNALG VALID ONLY ON GENCERT) . ++VER (Z038) FMID (CAKOF00) PRE (RO20497 RO23523 RO25900 RO35644 RO36198 RO40240 RO63150 RO63740 RO64503) SUP (TR63862 TR67882 TR68057) ++HOLD (RO68057) SYSTEM FMID(CAKOF00) REASON (DYNACT) DATE (14062) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Only allow the SIGNALG parm on GENCERT and RENEWAL | +----------+----------+ |USERS | Clients that issue Digital Certificate commands. | |AFFECTED | | +----------+----------+ |KNOWLEDGE | 1- Product Administration 3- z/OS Systems Programming | |REQUIRED | 2- SMP/e 4- Security Administration | +----------+----------+ |ACCESS | SMP/e CSI libraries | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** SMP APPLY, LLA REFRESH and a restart of TSS,,,REINIT).

Release	Service	Details
15.0	RO68239	RO68239 M.C.S. ENTRIES = ++PTF (RO68239) SUPPORT MIRRORED SECURITY FILE PROBLEM DESCRIPTION: This solution introduces a new mirrored security file enhancement. This enhancement can only be leveraged if SHRFILE(NO) is set. In addition to this solution, the mirrored feature requires a new control option to be set. Without both requirements, implementation of this solution will have no impact on existing product functionality. When the MIRROR control option is activated, the CA Top Secret product maintains a mirror copy of the primary security file. The mirror file is an exact duplicate of the primary security file and provides an up-to-the-minute mirrored security file in the event of a sudden problem with the primary file. Prior to this feature, when the security file becomes degraded or unavailable due to various error conditions, a forward recovery procedure was necessary to update and activate a backup file so that it is current from the last executed CA Top Secret backup. The mirror file option can eliminate the need for this forward recovery procedure by allowing a restart of the CA Top Secret address space pointing to the mirrored file. In addition, having a mirror file available allows greater flexibility for when to schedule backup processing. For example, this allows you to run a CA Top Secret backup once per weekend when production system workloads are less likely to be impacted. As noted above, the mirror option can only be leveraged when SHRFILE is set to NO. If SHRFILE(YES) is set, and the MIRROR parameter is set to to MIRROR(ON), the following messages will result at startup: TSS9247E Mirror File not supported with Shared Secfile TSS9248I Security file Mirroring is Disabled SYMPTOMS: Delays in the security file availability to process work. IMPACT: Delays in switching from the primary security file to an updated and current alternate file. In addition, certain types of security services can timeout while a CA Top Secret backup is underway. CIRCUMVENTION: Until the MIRROR enhancement is implemented, there is no circumvention to eliminate the time necessary to run forward recovery. Until the Mirror file can be used in lieu of a daily backup, certain workloads impacted while the backup is running will be delayed or need to be rescheduled if a timeout condition has occurred. PRODUCT(S) AFFECTED: CA-TOP SECRET-MVS Release 15.0 Star Problem(s): TSSMVS 9513 Copyright (C) 2014 CA. All rights reserved. R00953-TSS150-SP1 DESC(SUPPORT MIRRORED SECURITY FILE) . ++VER (Z038) FMID (CAKOF00) PRE (RO18784 RO25587 RO26450 RO32653 RO35644 RO36198 RO37109 RO37235 RO38472 RO42576 RO43262 RO45811 RO47730 RO48248 RO48562 RO50925 RO55678 RO58366 RO60611 RO63150 RO63740 RO66142 RO67514) SUP (AR41767 CC56243 DC56243 RI63057 RO24363 RO26651 RO28221 RO28502 RO38053 RO40589 RO41151 RO41767 RO42155 RO42988 RO45152 RO45566 RO48278 RO48724 RO48727 RO50024 RO50143 RO52334 RO58021 RO58318 RO59441 RO63014 RO65763 TR16265 TR16707 TR16732 TR18055 TR24214 TR24363 TR26651 TR28221 TR28502 TR31112 TR31438 TR31827 TR32201 TR34459 TR34711 TR36584 TR38053 TR40589 TR41151 TR41664 TR41767 TR42155 TR42988 TR45152 TR45566 TR46685 TR47373 TR48278 TR48614 TR48724 TR48727 TR50024 TR50143 TR52334 TR57058 TR57652 TR58021 TR58318 TR59441 TR60294 TR63014 TR65763 TR66461 TR68239) ++HOLD (RO68239) SYSTEM FMID(CAKOF00)

Release	Service	Details
		REASON (DYNACT) DATE (14119) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Support security file mirror files. | +----------+----------+ |USERS | All | |AFFECTED | | +----------+----------+ |KNOWLEDGE | 1- Product Administration 3- z/OS Systems Programming | |REQUIRED | 2- SMP/e 4- Security Administration | +----------+----------+ |ACCESS | SMP/e CSI libraries | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** SMP APPLY, LLA refresh, and restart TSS required to install this APAR.). ++HOLD (RO68239) SYSTEM FMID(CAKOF00) REASON (DOC) DATE (14119) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ ********** * PUBLICATION * ********** THE FOLLOWING CA TOP SECRET GUIDES HAVE BEEN UPDATED RELATEED TO THIS support. Access to these updated guides is available via CA Support Online. Each guide (just prior to the start of the CONTENTS section) has a DOCUMENTATION CHANGES section that provides hyper links to the related new feature documentation updates. CA Top Secret Release Notes Guide CA Top Secret Command Functions Guide CA Top Secret Control Options Guide CA Top Secret Report and Tracking Guide CA Top Secret Message Reference Guide).

Release	Service	Details
15.0	RO68361	RO68361 M.C.S. ENTRIES = ++PTF (RO68361) AUTOUID IMPROPERLY SENT TO PASSWORD-ONLY NODES PROBLEM DESCRIPTION: With CPFAUTOUID or CPFAUTOGID enabled (with RO63150 implemented), UIDs and/or GIDs added automatically via the UNIQUSER feature or via the TSS ADD() UID(?) GID(?) command, can be improperly routed to password-only CPF nodes. SYMPTOMS: UIDs and GIDs will be improperly added or replaced on the password-only target nodes. IMPACT: The impact is site specific. If UIDs or GIDs are duplicated across multiple nodes for different users/groups these fields may be overlaid on the nodes which do not expect to receive these commands. CIRCUMVENTION: Do not enable UNIQUSER with CPFAUTOUID or CPFAUTOGID if Password-Only nodes are defined. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9565 Copyright (C) 2014 CA. All rights reserved. R00957-TSS150-SP1 DESC(AUTOUID IMPROPERLY SENT TO PASSWORD-ONLY NODES) . ++VER (Z038) FMID (CAKOF00) PRE (RO18634 RO19256 RO20497 RO21793 RO23523 RO25900 RO35644 RO36198 RO37109 RO38472 RO46203 RO50801 RO53633 RO55678 RO63150 RO63740 RO63941) SUP (TR16894 TR16956 TR17040 TR17122 TR17596 TR18880 RO18880 TR20230 RO20230 TR20898 RO20898 TR21191 RO21191 TR28526 RO28526 TR28778 RO28778 TR29757 TR32792 RO32792 TR33282 RO33282 TR38385 TR33505 TR33519 TR38784 TR38899 RO38385 RO38784 RO38899 TR49662 RO49662 TR57685 RO57685 TR59203 RO59203 TR59314 KR55678 RO59314 TR65717 AR63740 RO65717 TR65891 RO65891 TR67089 RO67089 TR68361 CR63150) ++HOLD (RO68361) SYSTEM FMID(CAKOF00) REASON (DYNACT) DATE (14085) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Load module into LLA and activate | +----------+----------+ |USERS | All users of CA Top Secret | |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).

Release	Service	Details
15.0	RO68393	RO68393 M.C.S. ENTRIES = ++PTF (RO68393) AT TIMES THE DFLTGRP NOT ADDED TO THE GROUP LIST PROBLEM DESCRIPTION: After fix RO67810, the DFLTGRP may not be added to the group list, depending on the return code from the lookup subroutine. SYMPTOMS: The DFLTGRP is not added to the list of groups for the acid. The error received depends on the application. Customers using FTP have reported the following error: FTPSTEP - ABEND=S000 U4093 REASON=00000090 IMPACT: Applications dependent on INITUSP functionality may terminate with errors. CIRCUMVENTION: Manually add OMVS segment fields, GROUP and DFLTGRP to the ACID for which INITUSP previously failed. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9566 Copyright (C) 2014 CA. All rights reserved. R00958-TSS150-SP1 DESC(AT TIMES THE DFLTGRP NOT ADDED TO THE GROUP LIST) . ++VER (Z038) FMID (CAKOF00) PRE (RO55678 RO61359 RO63740) SUP (CR63740 RO54316 RO67810 TR54316 TR66462 TR66605 TR67221 TR67801 TR67810 TR68393 AR67810) ++HOLD (RO68393) SYSTEM FMID(CAKOF00) REASON (DYNACT) DATE (14112) COMMENT (+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Correct error adding DFLTGRP as GROUP on user. | +----------+----------+ |USERS | All users that leverage UNIQUSER and MODLUSER. | |AFFECTED | | +----------+----------+ |KNOWLEDGE | 1- Product Administration 3- z/OS Systems Programming | |REQUIRED | 2- SMP/e 4- Security Administration | +----------+----------+ |ACCESS | SMP/e CSI libraries | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** SMP APPLY, LLA REFRESH, TSS,,,REINIT to install this APAR.).

Release	Service	Details
15.0	RO68435	RO68435 M.C.S. ENTRIES = ++PTF (RO68435) ABEND S0C4 IN TSSAUTHA ON REFRESH JOBNAME(*) PROBLEM DESCRIPTION: An S0C4 abend in TSSAUTHA can occur when a TSS REFRESH command is issued with keyword JOBNAME(*) to refresh all occurances of a user in all address spaces. The abend is intermittent and occurs when a targeted address space is in transition from active to inactive and required control blocks are no longer available. SYMPTOMS: TSS9999E CA-TSS SECURITY SVC ABEND S0C4 IN TSSAUTHA+3846 The issuer of the TSS REFRESH command will receive the message and the command execution will terminate. IMPACT: Not all users that were the target of the command will have their security environment refreshed. CIRCUMVENTION: Users will have to refresh their own security environment with a TSS REFRESH command issued locally. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9532 Copyright (C) 2014 CA. All rights reserved. R00959-TSS150-SP1 DESC(ABEND S0C4 IN TSSAUTHA ON REFRESH JOBNAME(*)) . ++VER (Z038) FMID (CAKOF00) PRE (RO25119 RO32654 RO36198 RO57887) SUP (TR16903 TR37192 TR38282 BR63150 RI66832 RO37192 RO38282 TR28680 TR66033 TR66833 RO66833 TR68435) ++HOLD (RO68435) SYSTEM FMID(CAKOF00) REASON (DYNACT) DATE (14097) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Resolve 0C4 abend in TSSAUTHA with REFRESH JOBNAME(*) | +----------+----------+ |USERS | Administrators attempting to refresh security permissions | |AFFECTED | for a user in multiple address spaces. | +----------+----------+ |KNOWLEDGE | 1 - SMP/E | |REQUIRED | 2 - z/OS Systems Programming | | | 3 - Security Administration | +----------+----------+ |ACCESS | SMP/E CSI Libraries | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** 1. F LLA,REFRESH 2. Recycle using TSS,,,REINIT).

Release	Service	Details
15.0	RO68831	RO68831 M.C.S. ENTRIES = ++PTF (RO68831) TSSAUDIT RETURN CODE PROCESSING PROBLEM DESCRIPTION: TSSAUDIT UTILITY improperly passes return code 0 for invalid parms. For example, running TSSAUDIT with CHANGES(-7) parameter, should produce the following error message but does not: TSS8125E OPTION UNKNOWN OR INVALID SYMPTOMS: None. IMPACT: Clients may believe TSSAUDIT worked when it actually failed. CIRCUMVENTION: None. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9568 Copyright (C) 2014 CA. All rights reserved. R00961-TSS150-SP1 DESC(TSSAUDIT RETURN CODE PROCESSING) . ++VER (Z038) FMID (CAKOF00) PRE (RO64503) SUP (AR24362 AR64503 RO24362 RO46218 RO49435 RO53949 RO67302 TR24362 TR46218 TR49435 TR53949 TR67302 TR68831) ++HOLD (RO68831) SYSTEM FMID(CAKOF00) REASON (DYNACT) DATE (14092) COMMENT (+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Load module into LLA and activate | +----------+----------+ |USERS | All users of CA Top Secret | |AFFECTED | | +----------+----------+ |KNOWLEDGE | 1. Console commands | |REQUIRED | | +----------+----------+ |ACCESS | 1. Console authority | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** SMP APPLY, LLA REFRESH and rerun TSSAUDIT).

Release	Service	Details
15.0	RO69065	RO69065 M.C.S. ENTRIES = ++PTF (RO69065) OVERLAY OF CSA WITH PKISERV AND OPTION(32) ACTIVE PROBLEM DESCRIPTION: CSA can be overlaid when CA Control Option options(32) is active for logging USS events to the Audit Tracking File. The Overlay occurs when the log record is greater than x'1D0' in length. SYMPTOMS: This problem has been reported during r_PKIServ function QUERYCERTS calls. So far the storage that has been overlaid has been reported to cause DB2, VTAM and NETVIEW to ABEND. IMPACT: The circumstances necessary for this problem to occur require OPTIONS(32) to be active. The primary problem is a storage overlay. The results are somewhat unpredictable but can be severe enough to require an IPL. CIRCUMVENTION: Disable OPTIONS(32) until this maintenance is applied. To disable you must remove the setting from the parameter file and restart CA Top Secret. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Release 14.0 Star Problem(s): TSSMVS 9571 Copyright (C) 2014 CA. All rights reserved. R00964-TSS150-SP1 DESC(OVERLAY OF CSA WITH PKISERV AND OPTION(32) ACTIVE) . ++VER (Z038) FMID (CAKOF00) SUP (TR69065 JC56243) ++HOLD (RO69065) SYSTEM FMID(CAKOF00) REASON (DYNACT) DATE (14101) COMMENT (+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Load module into LLA and activate | +----------+----------+ |USERS | Client that have Option(32) active | |AFFECTED | | +----------+----------+ |KNOWLEDGE | 1- Product Administration 3- z/OS Systems Programming | |REQUIRED | 2- SMP/e 4- Security Administration | +----------+----------+ |ACCESS | SMP/E CSI Libraries | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** SMP APPLY, LLA REFRESH, TSS,,,REINIT).