Release	Service	Description	Hiper
15.0	RO58367	SECCACHE CLEARING PREMATURELY	
	RO63941	PERMITTING FORCE ON REMOVE OF CERTIFICATE	
	RO64815	DFHUS0002 ERROR (CODE X'030C') W/OPTIONS(20)	
	RO65451	USING AES ENCRYPT PASSWORD 378-14 IN TSSAENCR	
	RO65662	OMVS SIGNON MAY BUILD INCORRECT GROUPLST AFTER RO61359	
	RO65717	NO CASECAUT BY TYPE USER ON TSS MODIFY	
	RO66128	AFTER RO64969 NON-DATASET TRACES REMAIN DISABLED	
The CA RS 1401 service count for this release is 7			

Release	Service	Description	Hiper
14.0	NO-SRVC	CA RS 1401 Contains No Service For This Release of This Product.	
The CA RS 1401 service count for this release is 0			

FMID	Service	Description	Hiper
CAKOF00	RO58367	SECCACHE CLEARING PREMATURELY	
	RO63941	PERMITTING FORCE ON REMOVE OF CERTIFICATE	
	RO65451	USING AES ENCRYPT PASSWORD 378-14 IN TSSAENCR	
	RO65662	OMVS SIGNON MAY BUILD INCORRECT GROUPLST AFTER RO61359	
	RO65717	NO CASECAUT BY TYPE USER ON TSS MODIFY	
	RO66128	AFTER RO64969 NON-DATASET TRACES REMAIN DISABLED	
The CA RS 1401 service count for this FMID is 6			

FMID	Service	Description	Hiper
CAKOF01	RO64815	DFHUS0002 ERROR (CODE X'030C') W/OPTIONS(20)	
The CA RS 1401 service count for this FMID is 1			

Release	Service	Details
15.0	RO58367	RO58367 M.C.S. ENTRIES = ++PTF (RO58367) SECCACHE CLEARING PREMATURELY PROBLEM DESCRIPTION: If SECCACHE(SIZE=2048) is used to set the size to the maximum allowed, an error in calculating the percentage of data in use results in attempting to clear expired entries every timer interval once the percentage reaches 1% rather than when the percentage reaches the warning threshold. This problem does not happen if the SECCACHE size is set to any value less than 2048. SYMPTOMS: The SECCACHE stats will show an increasing number of 'Deletes' even though neither the '% Used' value for both data and index have never been as high as the 'Warn %' value. IMPACT: The SECCACHE will be cleared too soon, leading to utilization being less than intended and performance improvements being less than what might be possible. CIRCUMVENTION: Use a smaller value for SIZE, such as SIZE=2047 PRODUCT(S) AFFECTED: CA-TOP SECRET-MVS Release 15.0 Star Problem(s): TSSMVS 9433 Copyright (C) 2013 CA. All rights reserved. R00784-TSS150-SP1 DESC(SECCACHE CLEARING PREMATURELY) . ++VER (Z038) FMID (CAKOF00) PRE (RO55678) SUP (TR58367) ++HOLD (RO58367) SYSTEM FMID(CAKOF00) REASON (ACTION) DATE (13312) COMMENT (+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Address SECCACHE being cleared prematurely. | +----------+----------+ |USERS | | |AFFECTED | All users that leverage the TSS SECCACHE | +----------+----------+ |KNOWLEDGE | 1- Product Administration 2- SMP/E | |REQUIRED | 3- z/OS Systems Programming 4- Security Administration | +----------+----------+ |ACCESS | | |REQUIRED | SMP/E CSI libraries | +----------+----------+ ********** * STEPS TO PERFORM * ********** SMP APPLY, LLA REFRESH and a restart of TSS with REINIT is required to install this APAR.).

Release	Service	Details
15.0	RO63941	RO63941 M.C.S. ENTRIES = ++PTF (RO63941) PERMITTING FORCE ON REMOVE OF CERTIFICATE PROBLEM DESCRIPTION: Certificate with an invalid private key in CSF cannot be removed from TSS database. This problem has shown up when one copied the security file from one system to another, when digital certificate keys were stored in the CSF. One was not able to remove the certificates from the copied file on the new system. Now one will be able to specified on the REMOVE command 'FORCE' which will allow one to bypass the CSF checking of the private key. SYMPTOMS: So far when one tried to issue TSS REMOVE(XXXX) DIGICERT(XXXXXX) one received 'CAS20E0E ICSF CSNDKRD service error - RC=8 RSN=16032'. IMPACT: The Digital Certificate is not removed. CIRCUMVENTION: If the security file is being clone to another system, be aware that until the maintenance is applied the certificate can not be removed. Star Problem(s): TSSMVS 9502 SUBJECTN WITH 1024 LENGTH GETS MESSAGE TSS0244E PROBLEM DESCRIPTION: When a GENCERT is issued with a SUBJECTN parameter whose length is 1024 characters, the command is failed when SIGNWITH is also specified. The limit is 1007 when there is no SIGNWITH. SYMPTOMS: GENCERT gets message TSS0244E. IMPACT: GENCERT command fails. CIRCUMVENTION: Use shorter SUBJECTN parameter. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9422 Copyright (C) 2013 CA. All rights reserved. R00874-TSS150-SP1 DESC(PERMITTING FORCE ON REMOVE OF CERTIFICATE) . ++VER (Z038) FMID (CAKOF00) PRE (RO18634 RO19256 RO20497 RO21793 RO23523 RO25900 RO35644 RO36198 RO37109 RO38472 RO46203 RO50801 RO53633 RO55678 RO63150 RO63740) SUP (RO18880 RO20230 RO20898 RO21191 RO28526 RO28778 RO32792 RO33282 RO38385 RO38784 RO38899 RO49662 RO57685 RO59203 RO59314 TR16894 TR16956 TR17040 TR17122 TR17596 TR18880 TR20230 TR20898 TR21191 TR28526 TR28778 TR29757 TR32792 TR33282 TR33505 TR33519 TR38385 TR38784 TR38899 TR49662 TR55073 TR55074 TR57685 TR59203 TR59314 TR63941) ++HOLD (RO63941) SYSTEM FMID(CAKOF00) REASON (ACTION) DATE (13315) COMMENT (+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ +----------+----------+ |SEQUENCE | AFTER APPLY | +----------+----------+ |PURPOSE | Permitting FORCE on remove of certificate. | +----------+----------+ |USERS | | |AFFECTED | All users that leverage TSS. | +----------+----------+ |KNOWLEDGE | 1- Product Administration 2- SMP/E | |REQUIRED | 3- z/OS Systems Programming 4- Security Administration |

Release	Service	Details
		+----------+--+ |ACCESS | | |REQUIRED | SMP/E CSI libraries | +----------+--+ ********** * STEPS TO PERFORM * ********** SMP APPLY, LLA REFRESH and a restart of TSS with REINIT is required to install this APAR.).

Release	Service	Details
15.0	RO64815	RO64815 M.C.S. ENTRIES = ++PTF (RO64815) DFHUS0002 ERROR (CODE X'030C') W/OPTIONS(20) PROBLEM DESCRIPTION: After CA Top Secret r15 PTF RO60786, with control option OPTIONS(20) set and facility matrix DEFACID defined with a userid that is 7 characters, a signon with an UNDEFINED userid of 8 characters will result in the cics region abending with: DFHUS0002 xxxxxxxx A severe error (code X'030C') has occurred in module DFHUSAD. SYMPTOMS: CICS ADENDS with the following message: DFHUS0002 xxxxxxxx A severe error (code X'030C') has occurred in module DFHUSAD. IMPACT: The CICS region ABENDS and will require a restart. CIRCUMVENTION: Remove OPTIONS(20) from TSS startup parameter file or DEFACID from cics facility matrix. PRODUCT(S) AFFECTED: CA-TOP SECRET-MVS Release 15.0 Star Problem(s): TSSMVS 9512 Copyright (C) 2013 CA. All rights reserved. R00888-TSS150-SP1 DESC(DFHUS0002 ERROR (CODE X'030C') W/OPTIONS(20)) . ++VER (Z038) FMID (CAKOF01) PRE (RO25588 RO26389 RO32608 RO43979 RO44835 RO53625) SUP (AR44835 TR58630 TR58760 TR58889 BR44835 RO58889 TR60786 RO60786 TR64815 AR60786) ++HOLD (RO64815) SYSTEM FMID(CAKOF01) REASON (ACTION) DATE (13312) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE |DFHUS0002 ERROR(CODE X'030C') W/OPTIONS(20) | +----------+----------+ |USERS |All users that levarege CICS with OPTIONS(20) and a | |AFFECTED |FACILITY MATRIX DEFACID. | +----------+----------+ +----------+----------+ | CA Top Secret for z/OS CICS Component Release 15.0 | |REQUIRED |2- SMP/e 4- Security Administration | +----------+----------+ |ACCESS | SMP/e CSI libraries | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** SMP APPLY, LLA REFRESH and a restart of CICS region is required to install this APAR.).

Release	Service	Details
15.0	RO65451	RO65451 M.C.S. ENTRIES = ++PTF (RO65451) USING AES ENCRYPT PASSWORD 378-14 IN TSSAENCR PROBLEM DESCRIPTION: After RO55678, an S378-14 ABEND in module TSSAENCR is possible when an invalid password length is passed on the RACROUTE VERIFY call. The ABEND occurs when AES ENCRYPTION is active for a security file. SYMPTOMS: Reported in CICS: Abend S378-14/AKEX occurred at offset X'0A*A' in DFHXSPW. IMPACT: The signon event will fail, region continues to function. CIRCUMVENTION: Ensure passwords are entered for all signon attempts. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9518 Copyright (C) 2013 CA. All rights reserved. R00901-TSS150-SP1 DESC(USING AES ENCRYPT PASSWORD 378-14 IN TSSAENCR) . ++VER (Z038) FMID (CAKOF00) PRE (RO55678) SUP (TR65451 JR55678) ++HOLD (RO65451) SYSTEM FMID(CAKOF00) REASON (ACTION) DATE (13336) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | To prevent S378-14 using AES pasword with invalid length | +----------+----------+ |USERS | User that have AES encryption active | |AFFECTED | | +----------+----------+ |KNOWLEDGE | 1 - SMP/E | |REQUIRED | 2 - z/OS Systems Programming | | | 3 - CICS 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	RO65662	RO65662 M.C.S. ENTRIES = ++PTF (RO65662) OMVS SIGNON MAY BUILD INCORRECT GROUPLST AFTER RO61359 PROBLEM DESCRIPTION: After CA Top Secret r15 PTF RO61359, when starting an OMVS session, the groups list can be incorrectly built and assigned to the user. This can occur when all three of the following conditions are present: 1) OMVS user does not have a DFLTGRP pre-assigned 2) Control Option OMVSGRP is set to OMVSGRP(*NONE*) 3) Control Option UNIQUSER is set to UNIQUSER(ON) SYMPTOMS: Group incorrectly assigned when starting an OMVS session. IMPACT: User may not be able to start OMVS session. CIRCUMVENTION: Manually assign DFLTGRP to user before starting OMVS session. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 TSS R15.0 Star Problem(s): TSSMVS 9521 Copyright (C) 2013 CA. All rights reserved. R00904-TSS150-SP1 DESC(OMVS SIGNON MAY BUILD INCORRECT GROUPLST AFTER RO61359) . ++VER (Z038) FMID (CAKOF00) PRE (RO58980 RO61359) SUP (TR65662 AR61359) ++HOLD (RO65662) SYSTEM FMID(CAKOF00) REASON (ACTION) DATE (13344) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | | | |Address incorrect GROUPLST built after RO61359. | | | | +----------+----------+ |USERS | | |AFFECTED | | | |OMVS users without DFLTGRP and OMVSGRP(*NONE*) | | |and UNIQUSER(ON) | | | | +----------+----------+ |KNOWLEDGE | | |REQUIRED | | | |1 - SMP/E | | |2 - z/OS Systems Programming | | |3 - CICS Systems Programming | | |4 - Security Administration | | | | +----------+----------+ |ACCESS | | |REQUIRED | | | |SMP/E CSI Libraries | | | | +----------+----------+ ********** * STEPS TO PERFORM * ********** 1. LLA Refresh

Release	Service	Details
		2. F TSS,REFRESH(SAF)).

Release	Service	Details
15.0	RO65717	RO65717 M.C.S. ENTRIES = ++PTF (RO65717) NO CASECAUT BY TYPE USER ON TSS MODIFY PROBLEM DESCRIPTION: After CA Top Secret r15 PTF RO55678, an acid of TYPE=USER with no CONSOLE authority can issue a 'TSS MODIFY' command, without a TYPE=CASECAUT RESOURCE=TSSCMD.ADMIN.MODIFY security call. An acid of TYPE=USER cannot modify/change any control options, they can only list out the control options. SYMPTOMS: An acid of TYPE=USER can issue a 'TSS MODIFY' command. IMPACT: Unauthorized acid's can view 'TSS MODIFY(ST)' output. CIRCUMVENTION: None. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9523 Copyright (C) 2013 CA. All rights reserved. R00905-TSS150-SP1 DESC(NO CASECAUT BY TYPE USER ON TSS MODIFY) . ++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 RO59314 TR65717 KR55678) ++HOLD (RO65717) SYSTEM FMID(CAKOF00) REASON (ACTION) DATE (13340) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE |Address the lack of a CASECAUT call on a TSS MODI command | +----------+----------+ |USERS |All user's issuing a TSS MODI command. | |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 with REINIT is required to install this APAR.).

Release	Service	Details
15.0	RO66128	RO66128 M.C.S. ENTRIES = ++PTF (RO66128) AFTER RO64969 NON-DATASET TRACES REMAIN DISABLED PROBLEM DESCRIPTION: After RO64969, SAF trace without DSN will start but remain disabled. It can not be enabled. SYMPTOMS: No trace records are produced. The CAS2110I SECTRACE SET message is issued. IMPACT: No trace records. The trace must be rerun. CIRCUMVENTION: Restart the trace with DSN. PRODUCT(S) AFFECTED: CA Top Secret for z/OS Release 15.0 Star Problem(s): TSSMVS 9535 Copyright (C) 2013 CA. All rights reserved. R00918-TSS150-SP1 DESC(AFTER RO64969 NON-DATASET TRACES REMAIN DISABLED) . ++VER (Z038) FMID (CAKOF00) SUP (TR64969 RO64969 TR66128 AR64969) ++HOLD (RO66128) SYSTEM FMID(CAKOF00) REASON (ACTION) DATE (13353) COMMENT (+----------+----------+ | CA Top Secret for z/OS Release 15.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | Produce SAF trace records when DSN= not specified | +----------+----------+ |USERS | Users that run SAF trace. | |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 refresh SAFTRRVT with F TSS,REFRESH(TRRVT) is required to install this APAR.).