CA Common Services 14.1
CA RS 1603 Service List

Release	Service	Description	Type
14.1	RO85819	CAUNZIP FAILS IF ZIPFILE IS MISSING THE EXTENSION	PTF
	RO88019	CAUNZIP GETS SECURITY VIOLATIONS ON TEMPORARY DATASETS	PTF
The CA RS 1603 service count for this release is 2			

FMID	Service	Description	Type
CAS9E10	RO85819	CAUNZIP FAILS IF ZIPFILE IS MISSING THE EXTENSION	PTF
	RO88019	CAUNZIP GETS SECURITY VIOLATIONS ON TEMPORARY DATASETS	PTF
The CA RS 1603 service count for this FMID is 2			

Release	Service	Details
14.1	RO85819	RO85819 M.C.S. ENTRIES = ++PTF (RO85819) CAUNZIP FAILS IF ZIPFILE IS MISSING THE EXTENSION PROBLEM DESCRIPTION: When CAUNZIP is executed against a ZIPFILE name that doesn't contain an extension (.ZIP, .ZP, .Z), CAUNZIP fails without producing any meaningful error message. When the allocation of a directory fails during CAUNZIP processing, CAUNZIP just reports that the allocation failed without any details about the failure. SYMPTOMS: In the case of a ZIPFILE without an extension, CAUNZIP produces message CAZIP20T Internal error without any additional details. In the case of an allocation failure, CAUNZIP produces message CAZIP02E without any reason for the failure, and terminates with return code 12. IMPACT: In the case of a ZIPFILE without an extension, CAUNZIP terminates with the CAZIP02T error message. In the case of an allocation failure, CAUNZIP terminates with the CAZIP02E error message. CIRCUMVENTION: In the case of a ZIPFILE without an extension, rename the ZIPFILE to contain an .ZIP extension and rerun the CAUNZIP utility. There is no circumvention for an allocation failure. PRODUCT(S) AFFECTED: CAUNZIP Release 14.1 Related Problem: CAIRIM 559 Copyright (C) 2016 CA. All rights reserved. R00385-AW0141-SP1 DESC(CAUNZIP FAILS IF ZIPFILE IS MISSING THE EXTENSION). ++VER (Z038) FMID (CAS9E10) PRE (RO54635 RO58216 RO62474) SUP (RO58379 RO68673 RO69320 RO82611 TR58379 TR68673 TR69320 TR82611 TR85819)

Release	Service	Details
14.1	RO88019	RO88019 M.C.S. ENTRIES = ++PTF (RO88019) CAUNZIP GETS SECURITY VIOLATIONS ON TEMPORARY DATASETS PROBLEM DESCRIPTION: Running CAUNZIP, customer has some RACF security messages on temporary datasets during the run. The security violation is against the dsns SYS16018.T133055.RA000.SPYDIS01.R0 and not against datasets with the TEMPHLQ qualifier. Further investigation reveals that when the user assigned to the job is also allowed to act as a superuser, CAUNZIP switches to superuser and creates these temporary datasets under the account of superuser (Uid(0)). When CAUNZIP ends, it switches back to the original UID of the user assigned to the job and this user is then NOT allowed to delete the temporary datasets. When he removes the superuser allowance of this user, and that userid is not allowed to run with UID(0), there are no security violation messages. SYMPTOMS: Message: ICH408I USER(********) GROUP(********) NAME(**********) SYS16018.T133055.RA000.********.R0A65404 CL(DATASET) VOL(******) INSUFFICIENT ACCESS AUTHORITY ACCESS INTENT(ALTER) ACCESS ALLOWED(NONE) IMPACT: CAUNZIP continues normally. CIRCUMVENTION: Run the CAUNZIP job with a user id that is NOT defined as a superuser. PRODUCT(S) AFFECTED: CAUNZIP Release 14.1 Related Problem: CAIRIM 563 Copyright (C) 2016 CA. All rights reserved. R00393-AW0141-SP1 DESC(CAUNZIP GETS SECURITY VIOLATIONS ON TEMPORARY DATASETS). ++VER (Z038) FMID (CAS9E10) PRE (RO54635 RO58216 RO62474) SUP (RO58379 RO68673 RO69320 RO82611 RO85819 TR58379 TR68673 TR69320 TR82611 TR85819 TR88019)