RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 10
Issue 4

October
2016

Password Disclosure in SMF

If a user accidentally enters a password when prompted to enter a USERID, an SMF type 80 JOBINIT for Undefined User record is generated and the password appears in the USERID field. An ICH408I USER(*password*) GROUP( ) NAME() LOGON/JOB INITIATION - USER AT TERMINAL *termid* NOT RACF DEFINED may also be displayed on the system log. If the user then logs on correctly from the same terminal, a second JOBINIT record may be generated, showing the user's ID. Anyone with access to SMF archives can search for undefined user logons followed by successful logons in an attempt to discover user passwords. Be sure to strictly limit READ access to SMF archives containing RACF records. (How many of us have trained our users to change their password if this happens?)

This issue presents a strong case for the use of Multi-Factor Authentication (MFA).

FDR & DASDVOL

If there is no DASDVOL profile protecting a DASD volume, anyone with access to the FDR backup can restore the volume.

AUTOMOUNT Security Issues

z/OS Unix automount enables a user's personal home directory to be stored in its own unique file system dataset which is automatically mounted when the user dubs into Unix. Mount points for automount are defined in the file /etc/auto.master. Mount options for these file systems are specified in associated NameMap files (e.g., /etc/u.map).

NameMap mount option *setuid* determines whether setuid is honored when the file system is mounted. By default, it is set to *Yes*, in which case programs in the file system with the setuid bit on execute with the Unix UID of the program's owner, not that of the user who invoked it. A program owned by UID 0 with the setuid bit on runs as Superuser. If users can change the contents of their file system datasets outside of Unix's control, as would be allowed if a user's personal file system dataset has the user's own ID as its High Level Qualifier, a clever user could change the owner of their programs to 0 and set their setuid bits on. Always specify *setuid No* in NameMap options for user home directory file systems.

NameMap mount option *allocany* directs Unix to create a user's z/OS file system dataset when one does not already exist. By default, the new file system's root directory permission bits are set to rwxr-x---. The UID of the user is made the owner. The GID of the user's default group is made the group. If your RACF group architecture is such that all users have the same default group, then all users will have r-x access to every other user's home directory. If this is not desirable, specify allocany's keyword *pathperm* to change the permission bits. We recommend *pathperm(700).*

For more on protecting z/OS Unix, attend RSH's RACF - Securing z/OS Unix course.

CA-TPX Logon Logging

By default, CA-TPX is not configured to log authorized logons. If you want all logons logged, contact CA Technologies. They can tell you how to access a hidden, undocumented administration panel where you can activate such logging via Reserved Option #28 - USE LOG=ALL FOR RACINIT, RACROUTE CALLS. Apply all CA-TPX maintenance before activating.

IRRDBU00 Record Sequence

As a general rule, detail records precede basic data records on the IRRDBU00 unload file. For example, Group member 0102 records appear before the Group 0100 basic data record itself. Records for segments (e.g., Group OMVS segment 0120) appear after the basic record.

Group member 0102 records are listed in the order the users were connected just as they would

appear in a LISTGRP command. Similarly, user member 0203 records are listed in the order the user was connected to the groups just as they would appear in a LISTUSER command. User connect detail 0205 records, however, are listed in group alphanumeric sequence.

Dataset access list 0402 and 0404 records and General Resource access list 0505 and 0507 records are listed in the order the users and groups were permitted access just as they would appear in LISTDSD or RLIST commands.

General Resource member 0503 records are listed in the order they were added to the profile; whereas, an RLIST command lists them in alphanumeric sequence. Understanding the actual sequence in which RACF members are stored in the profile can help with troubleshooting NODES and RACFVARS profiles.

SDSF / and ISFOPER.SYSTEM

SDSF is an Extended Multiple Console Support (EMCS) console, allowing SDSF users to enter z/OS operator commands. Most actions a user requests from an SDSF panel, such as cancelling a job, result in a command being automatically generated and executed on the user's behalf without the user being aware this is occurring.

A user can also enter z/OS commands from the command line within SDSF using SDSF's / command. To display OMVS information, the user would enter /D OMVS. To use the / command, the user must be permitted READ access to the SDSF resource ISFOPER.SYSTEM. The user must also be permitted access to the z/OS command via OPERCMDS profiles. In the example above, READ access to OPERCMDS resource MVS.DISPLAY.OMVS is required.

If the / command is entered by itself without an operator command, SDSF displays a panel much like Option 6 in ISPF. This enables the user to enter longer commands as well as to review and recall past commands. The authorization check for ISFOPER.SYSTEM access is not made until the user attempts to execute a z/OS command.

SDSF checks the user's OPERCMDS authority to use a z/OS command before execution. When the command is generated by an SDSF panel option, CONSOLE=SDSF is included in the RACROUTE call, enabling use of a WHEN(CONSOLE(SDSF)) conditional permission to allow execution only from within SDSF. CONSOLE=SDSF is not included when a z/OS command is entered via SDSF's / command, and the user must be given standard access permission to use the command.

EXEC.RACF.CLIST PDS

When you execute the SEARCH command with the CLIST operand, RACF creates a sequential dataset named *yourid*.EXEC.RACF.CLIST and writes the list of selected profiles to it with whatever before and after strings you specify. The dataset is allocated with RECFM=VB and LRECL=255. If the dataset already exists, RACF simply overwrites its contents.

If you pre-allocate this dataset as a PDS, SEARCH CLIST will create or overwrite a member in this PDS with the name TEMPNAME. To retain the set of commands, just rename TEMPNAME. To execute commands in a PDS member, append the member name to the dataset name:

EXEC '*yourid*.EXEC.RACF.CLIST(*member*)'

CEA and /var/CEAServer

CEA needs write to /var to perform an unlink. Set the permissions bits on /var to 1777. This is best done with a chmod command in the /etc/rc file.

RSH News

Support for z/OS 1.13 ended in September. Still need to replace the Unix Default User? Call us.

Thank you to all who respond to our surveys!