RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 12
Issue 4
October
2018

FTP JES Interface RFE

As described in our RACF Tips newsletter of April 2010, FTP allows users to submit batch jobs and retrieve SYSOUT from the JES spool. There are no FTP options or SAF calls to block or limit the use of this feature. Although such controls can be implemented using an exit (we have been able to do so with FTP's FTCHKCMD exit), exits are not a viable control option because few installations have the desire, technical know-how, or time needed to code and maintain them.

To address this issue, and in doing so counter a published Metasploit Framework exploit for abusing this interface, RSH submitted a Request for Enhancement (RFE) to improve controls for the FTP JES interface. The RFE ID is 125151, and the title is "Improved Security and Control for FTP JES Interface". IBM marked it "Private", so you will not be able to view or vote for it. If you agree with us that additional controls are needed and want to encourage IBM to act on this matter, we urge you to submit your own RFE. We will be happy to provide you with a copy of the verbiage we used for ours. Contact us if you want a copy.

For more on RFEs, read our January 2016 Tips.

Group Dataset Profile Owner

To assign a user as the owner of a group dataset profile, the user must be connected to the dataset's High Level Qualifier (HLQ) group. A user cannot be removed from a group if the user owns any dataset profiles related to that group.

RSH typically recommends a group be specified as the owner of a group dataset profile, preferably the group that matches the HLQ.

VSAM Access Check Bypass

If a user running either in Supervisor state or with storage protection key of 0 opens a VSAM file, the SAF access authorization check is bypassed.

DUMP FULL and DASDVOL

ADRDSSU is a storage administration utility used to backup, copy, and restore data.

The ADRDSSU command 'DUMP FULL' creates a 'physical' backup of an entire disk volume. If the command keyword ADMINISTRATOR or ADMIN is included, ADRDSSU does a RACF check to see if the user has READ access to FACILITY resource STGADMIN.ADR.STGADMIN.DUMP. If permitted access, the command executes with ADMIN authority. This powerful authority alone is sufficient to perform any backup operation.

Users without ADMIN authority can execute DUMP FULL if they have READ access to the DASDVOL profile protecting the volume. This applies to SMS-managed volumes as well.

The ADRDSSU documentation indicates that the DASDVOL check occurs after the ADMIN check and only when ADMIN authority was not granted. However, as we discovered during a recent OPERATIONS authority remediation effort, this is not the case. ADRDSSU still does the DASDVOL check, but it ignores the result.

An RFE exists to eliminate superfluous DASDVOL checks similar to this one. The RFE ID is 102423, and the title is "Remove DASDVOL call from DFDSS logical dataset dump". Please vote for it.

Permitting Temporary Access

To grant a user access to a resource on a temporary basis, create a group, permit the group access to the profile protecting the resource, and then connect the user to the group with a REVOKE date as shown below. Beginning on the date specified, the group connect will be ignored, and the access will no longer be allowed.

CO userid GROUP(group) REVOKE(mm/dd/yy)

We have used this feature to put time limits on fire-call type access. It can also be used to allow System Programmers UPDATE access to APF-authorized libraries for limited periods of time to perform upgrades or apply maintenance.

New STGADMIN Resources

The following FACILITY class STGADMIN-prefixed Storage Administration resources are relatively new.

STGADMIN.ADR.DUMP.CLOUD
STGADMIN.ADR.DUMP.ZCOMPRESS
STGADMIN.ADR.RESTORE.CLOUD
STGADMIN.ADR.SPACEREL
STGADMIN.ANT.ESS.OBJSTORE
STGADMIN.ARC.ENDUSER.HMIGRATE.CLOUD
STGADMIN.ARC.UPDTCDS
STGADMIN.IGG.CATALOG.SECURITY.CHANGE
STGADMIN.IGG.CATALOG.SECURITY.BOTH
STGADMIN.SMS.ALLOW.DATASET.ENCRYPT
STGADMIN.SMS.FAIL.INVALID.DSNTYPE.ENC

Users not permitted READ access to the resource whose name ends in .ENCRYPT cannot protect datasets using pervasive encryption, and those not permitted READ access to the one ending in .DSNTYPE.ENC can create unencrypted datasets when encryption fails. Give both UACC(READ).

Review your existing profiles to ensure these resources are properly protected.

For more on storage administration protection, attend our "RACF Level III" course.

BPX.STICKYSUG

If a user attempts to execute a program file that is residing in the Unix File System and the file has the Sticky bit on, z/OS Unix will not execute the file itself and will instead use the MVS program search order to find the program for execution (e.g. STEPLIB, JOBLIB, LNKLST).

If the Sticky bit program file has either the SETUID or SETGID bit on, which means the program will run with the authority of the file's owner UID or group GID, z/OS Unix will not search for an MVS program but will instead execute the program file itself. This avoids execution of a rogue MVS program that could misuse the SETUID and SETGID authority.

To override this control and execute an MVS program anyways, define a FACILITY class profile of BPX.STICKYSUG.*program-name*. The mere existence of such a profile is sufficient to activate the override. No permissions are needed.

Generic profiles can be used to override the control for multiple programs. For example, profile BPX.STICKYSUG.LPGM* applies to all programs whose names begin with LPGM.

To override the control for all programs, including those provided by IBM, define the following profile exactly as shown. *This is not recommended.*

BPX.STICKYSUG.*

Not stated clearly in the manuals is that any override profile must start with BPX.STICKYSUG., including the end period. A more generic profile such as BPX.** will not activate the override.

To learn more about protecting z/OS Unix, attend our "RACF - Securing z/OS Unix" course.

Auditors: SETROPTS

SETROPTS ("**SET** RACF **OPT**ION**S**") is a TSO command (a program) used to set and list RACF's configuration options. The options are stored in the first record of the RACF database, and they are usually referred to as the SETROPTS options. Execute command "SETROPTS LIST" to list the options. Note that options related to logging will not be displayed unless the user executing the command has AUDITOR or ROAUDIT authority.

Attend our course "RACF - Audit and Compliance Roadmap" for details on SETROPTS options.

RSH News

If you are the least bit uncertain as to how your system may be vulnerable to hacking, call us.

Tell your colleagues about our newsletter so they can get on our mailing list. There is a subscription form on our website's RACF Center webpage.

Be sure to attend RSH's RACF presentations at IBM's TechU in Hollywood, FL and at upcoming RACF User Group meetings.