IBM z/OS Authorized Code Scanner (zACS)

Technical Overview

THE EXCHANGE

Reaching Out to the z Community Worldwide

Bryan Childs
Solution Offering Manager
z/OS Security
bchilds@us.ibm.com

Use Cases for Cyber Resiliency are called Risks

$3.9M

Average cost of a data breach in 2019

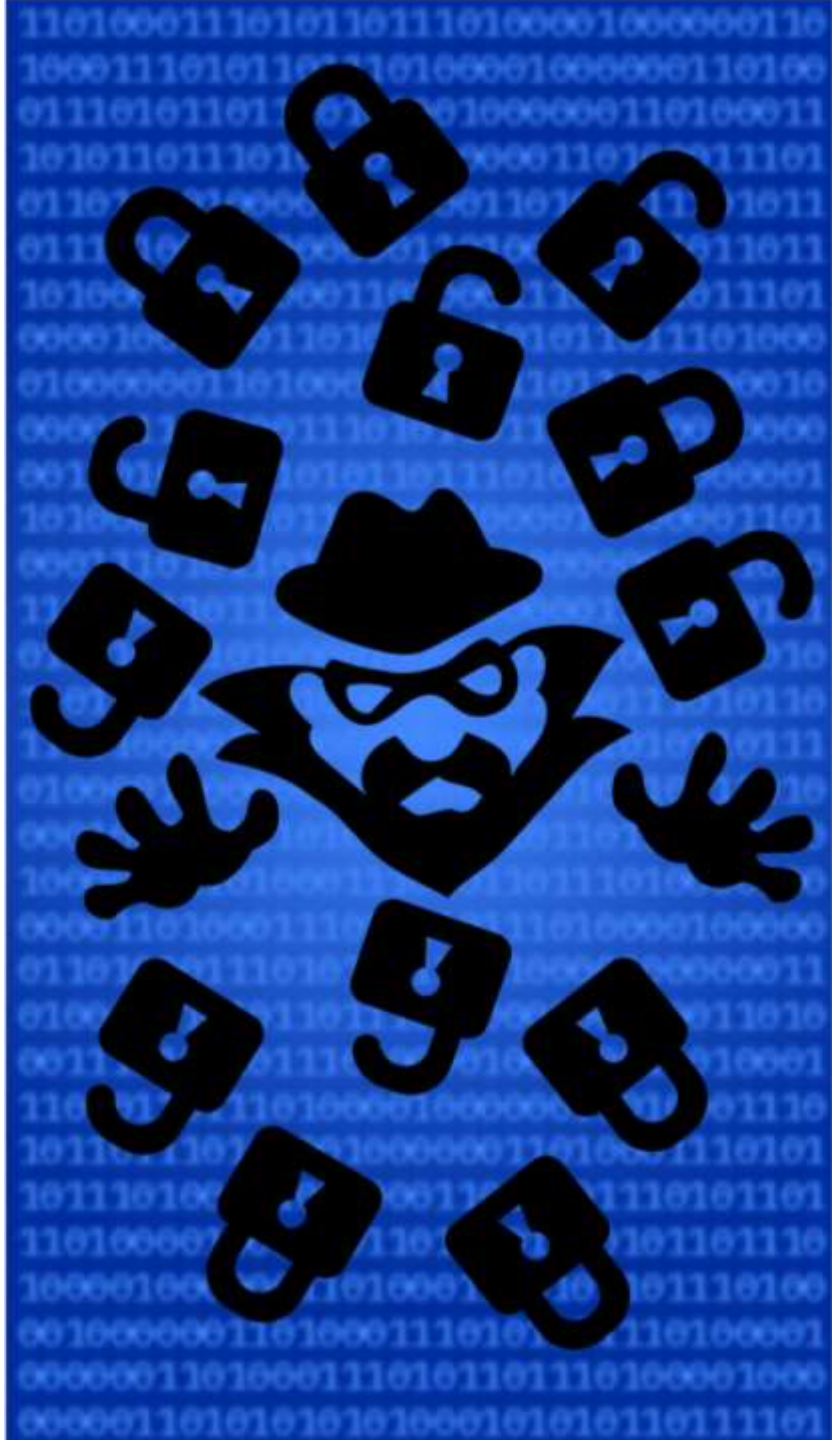
&

$150

cost per record

See the report:

http://www.ibm.com/security/data-breach



The IBM Z and LinuxONE Security Portal

IBM utilizes internal and external sources to uncover potential vulnerabilities. IBM Z offers a Security Portal that allows clients to stay informed about patch data, associated Common Vulnerability Scoring System (CVSS) ratings for new APARs and Security Notices to address highly publicized security concerns.

See more at: https://www.ibm.com/it-infrastructure/z/capabilities/system-integrity

Cyber Resiliency Guidance on Integrity

Keeping enterprise IT systems secure is critical. Pervasive Encryption on IBM Z, IBM RACF for z/OS, and IBM Z Multi-Factor Authentication are just a few examples of differentiating enterprise security function available on the IBM Z platform…

They all rely upon system integrity.

Authorized programs on z/OS and their associated application programming interfaces are critical to that integrity. These include authorized programs from:

- IBM
- The z/OS ecosystem
- In-house code specific to a client’s enterprise

Clarifying the Risk

The boundary between an unauthorized caller and a PC or SVC routine running Supervisor State Key 0 is critical to the System Integrity of the z/OS solution stack.

Parameter lists commonly have several levels of indirection. Each block of data must be safely copied or updated with specially architected instructions. Every block therefore constitutes a risk.

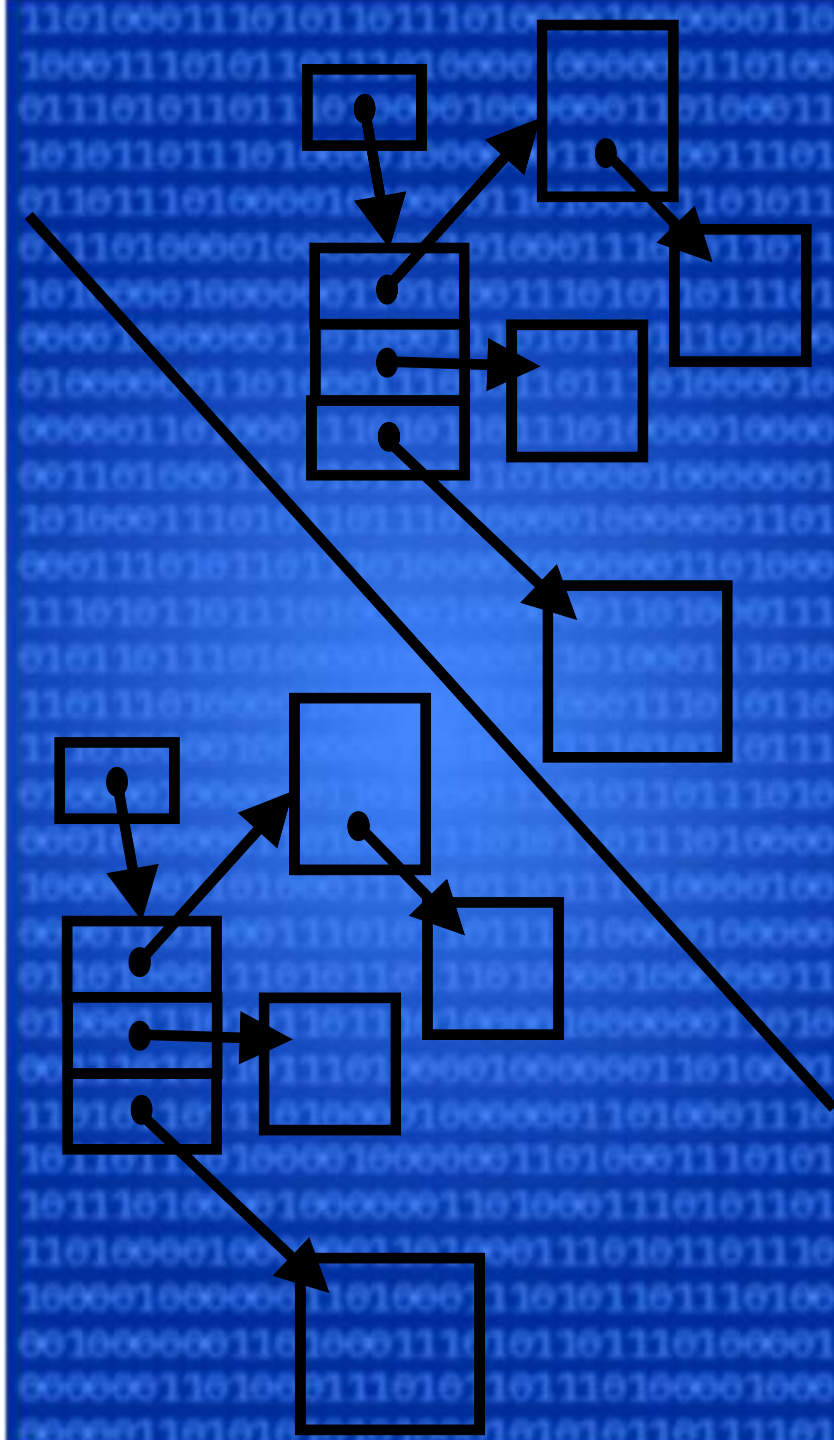
Any given z/OS image typically has hundreds of PCs & SVCs.

What’s the potential severity associated with this risk?

- CVSS 6.5 for a fetch-related vulnerability (“medium”)
- CVSS 8.8 for a store-related vulnerability (“high”)

(See https://www.first.org/)

There’s a need to discover vulnerabilities that might exist and remediate them, before they could be exploited.



IBM z/OS Authorized Code Scanner (zACS)

Authorized (critical) code needs a purpose-built scanner.

The IBM z/OS Authorized Code Scanner (zACS) is a new priced feature of z/OS version 2 release 4 created to help support clients in their efforts to strengthen the security posture of the z/OS dev/test pipeline. It dynamically scans the client's authorized code and provides diagnostic information for subsequent investigation as needed.

The scanner searches for potential vulnerabilities.

DevSecOps for z/OS applies to product upgrades, service, and in-house development. With lots of different teams involved in the process, this offering serves to strengthen the foundation of that dev/test pipeline and its increased pace, to help avoid potential compromise to the system integrity & security of the z/OS platform.

Parts & Externals

The IBM z/OS Authorized Code Scanner (zACS) consists of:

- REXX
- Batch
- Started Task

The input:

- Generated PC & SVC tables
- Syslog

The recommended output:

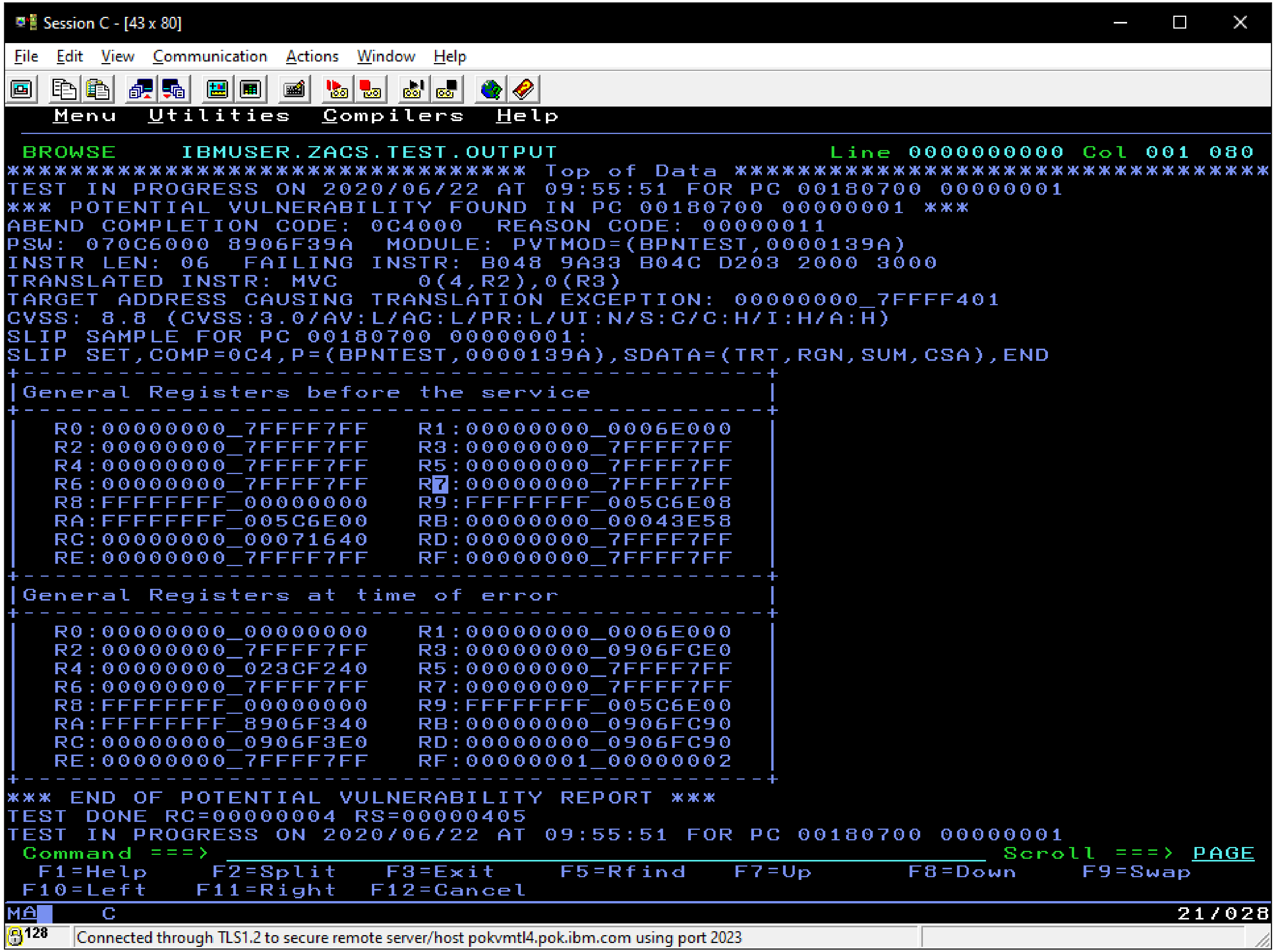
- Data Set

Running the Tool

The IBM z/OS Authorized Code Scanner (zACS) is run in the following steps:

1. Initialize the Started Task
2. Run the batch jobs to generate the PC & SVC tables
3. Run the REXX to generate test cases in batch
   - Run REXX directly or via ISPF panels
   - Optionally filter by inclusion or exclusion list
   - Wait for completion of the set

Sample Discovery Output



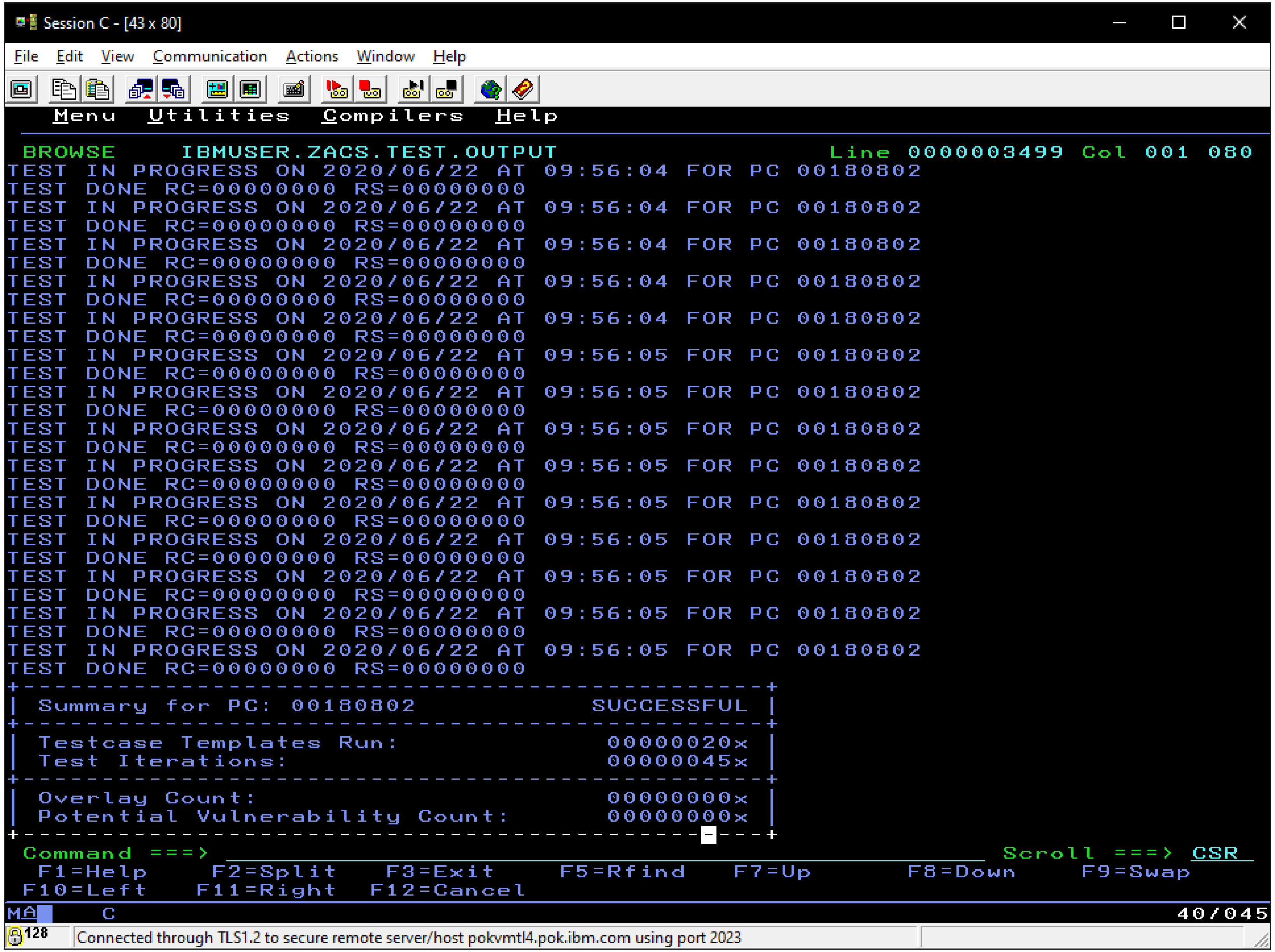
```
    Menu  Utilities  Compilers  Help

 BROWSE    IBMUSER.ZACS.TEST.OUTPUT                Line 0000000000 Col 001 080
********************************* Top of Data **********************************
TEST IN PROGRESS ON 2020/06/22 AT 09:55:51 FOR PC 00180700 00000001
*** POTENTIAL VULNERABILITY FOUND IN PC 00180700 00000001 ***
ABEND COMPLETION CODE: 0C4000  REASON CODE: 00000011
PSW: 070C6000 8906F39A  MODULE: PVTMOD=(BPNTEST,0000139A)
INSTR LEN: 06  FAILING INSTR: B048 9A33 B04C D203 2000 3000
TRANSLATED INSTR: MVC     0(4,R2),0(R3)
TARGET ADDRESS CAUSING TRANSLATION EXCEPTION: 00000000_7FFFF401
CVSS: 8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
SLIP SAMPLE FOR PC 00180700 00000001:
SLIP SET,COMP=0C4,P=(BPNTEST,0000139A),SDATA=(TRT,RGN,SUM,CSA),END
+-----------------------------------------------+
|General Registers before the service           |
+-----------------------------------------------+
|  R0:00000000_7FFFF7FF   R1:00000000_0006E000  |
|  R2:00000000_7FFFF7FF   R3:00000000_7FFFF7FF  |
|  R4:00000000_7FFFF7FF   R5:00000000_7FFFF7FF  |
|  R6:00000000_7FFFF7FF   R7:00000000_7FFFF7FF  |
|  R8:FFFFFFFF_00000000   R9:FFFFFFFF_005C6E08  |
|  RA:FFFFFFFF_005C6E00   RB:00000000_00043E58  |
|  RC:00000000_00071640   RD:00000000_7FFFF7FF  |
|  RE:00000000_7FFFF7FF   RF:00000000_7FFFF7FF  |
+-----------------------------------------------+
|General Registers at time of error             |
+-----------------------------------------------+
|  R0:00000000_00000000   R1:00000000_0006E000  |
|  R2:00000000_7FFFF7FF   R3:00000000_0906FCE0  |
|  R4:00000000_023CF240   R5:00000000_7FFFF7FF  |
|  R6:00000000_7FFFF7FF   R7:00000000_7FFFF7FF  |
|  R8:FFFFFFFF_00000000   R9:FFFFFFFF_005C6E00  |
|  RA:FFFFFFFF_8906F340   RB:00000000_0906FC90  |
|  RC:00000000_0906F3E0   RD:00000000_0906FC90  |
|  RE:00000000_7FFFF7FF   RF:00000001_00000002  |
+-----------------------------------------------+
*** END OF POTENTIAL VULNERABILITY REPORT ***
TEST DONE RC=00000004 RS=00000405
TEST IN PROGRESS ON 2020/06/22 AT 09:55:51 FOR PC 00180700 00000001
 Command ===>                                                  Scroll ===> PAGE
  F1=Help    F2=Split    F3=Exit     F5=Rfind    F7=Up       F8=Down     F9=Swap
 F10=Left   F11=Right   F12=Cancel
MA       C                                                               21/028
```

128
Connected through TLS1.2 to secure remote server/host pokvmtl4.pok.ibm.com using port 2023

Highlights:

- ABEND code & reason
- PSW
- Assembler translation
- Module & offset
- Target address
- Possible CVSS score
- SLIP sample
- General Regs
- Access Regs if applicable

Sample Summary



```
    Menu  Utilities  Compilers  Help
 ------------------------------------------------------------------------------
 BROWSE    IBMUSER.ZACS.TEST.OUTPUT                 Line 0000003499 Col 001 080
TEST IN PROGRESS ON 2020/06/22 AT 09:56:04 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:04 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:04 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:04 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:04 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:05 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:05 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:05 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:05 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:05 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:05 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:05 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:05 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
TEST IN PROGRESS ON 2020/06/22 AT 09:56:05 FOR PC 00180802
TEST DONE RC=00000000 RS=00000000
+------------------------------------------------+
| Summary for PC: 00180802            SUCCESSFUL |
+------------------------------------------------+
| Testcase Templates Run:              00000020x |
| Test Iterations:                     00000045x |
+------------------------------------------------+
| Overlay Count:                       00000000x |
| Potential Vulnerability Count:       00000000x |
+------------------------------------------------+
 Command ===>                                                  Scroll ===> CSR
  F1=Help    F2=Split   F3=Exit    F5=Rfind   F7=Up      F8=Down    F9=Swap
 F10=Left   F11=Right  F12=Cancel
MA      C                                                               40/045
```

128 Connected through TLS1.2 to secure remote server/host pokvmtl4.pok.ibm.com using port 2023

Summary Counts:

- Templates
- Testcases
- Overlays
- Vulnerabilities*

*Potential. False positives can occur. SLIP traces can be used for verification.

REXX Configuration, Part 1 of 4

```
/*******************************************************************/
/*                                                                 */
/* Runtime settings                                                */
/*                                                                 */
/* Instructions:                                                   */
/* Configure whether you would like to clear the logrec database   */
/*   while running zACS, default is 'NO'.                          */
/* Specify your logrec data set name.                              */
/* Choose the jobname you would like ZACS tests to run under,      */
/*   default is 'ZACSJ'.                                           */
/* Specify the MSGCLASS with which to submit testcase jobs, default */
/*   is 'A'.                                                       */
/* Specify 'LOG' to have the PC/SVC log data go to the log data sets */
/*   or 'SCREEN' to have it print to the screen, default is 'SCREEN'.*/
/*   Note: When using the panel, this value is ignored and output  */
/*   will go to the log.                                           */
/*                                                                 */
/*******************************************************************/
clearLogrec       = 'NO'
logrecDSname      = 'SYS1.LOGREC'
testcaseJobName   = 'ZACSJ'
jobMsgClass       = 'A'
printLogOutput    = 'SCREEN'
```

REXX Configuration, Part 2 of 4

```
/*******************************************************************/
/*                                                                 */
/* Filter settings                                                 */
/*                                                                 */
/* Instructions:                                                   */
/* Specify 'EXCLUDE' to exclude modules and/or jobnames during your */
/*   run or 'INCLUDE' to run a subset of modules and/or jobnames    */
/*   during your run. This value is ignored if both filterByModName */
/*   and filterByJobname are 'NO'. Default is 'EXCLUDE'.            */
/* Change 'module-name-filter-list-dataset' to the name of the      */
/*   data set containing the list of modules you would like to      */
/*   include or exclude. Configure whether or not you would like to */
/*   include or exclude modules during your run, default is 'NO'.   */
/* Change 'jobname-filter-list-dataset' to the name of the data set */
/*   containing the list of jobnames you would like to include or   */
/*   exclude. Configure whether or not you would like to include or */
/*   exclude jobnames during your run, default is 'NO'.             */
/*                                                                 */
/*******************************************************************/
includeOrExclude    = 'EXCLUDE'
filterByModName     = 'NO'
modFilterDSname     = 'module-name-filter-list-dataset'
filterByJobname     = 'NO'
jobFilterDSname     = 'jobname-filter-list-dataset'
```

REXX Configuration, Part 3 of 4

```
/*******************************************************************/
/*                                                   */
/* Vulnerability log setting                                   */
/*                                                   */
/* Instructions:                                           */
/* Change 'output-dataset' to the name of the data set to which you  */
/*   would like to send detected potential vulnerability output.     */
/*   This must match the data set name specified by MYOUTDD in the   */
/*   started task.                                         */
/* Specify 'ERROR' to suppress test in progress messages printed to  */
/*   the potential vulnerability log and to print return codes only  */
/*   when an unsuccessful result is detected. Specify 'ALL' to print */
/*   test in progress messages and to print return codes to the      */
/*   potential vulnerability log always. Default is 'ALL'           */
/* Specify 'ERROR' to suppress the summary information printed at    */
/*   the end of each service in the potential vulnerability log when */
/*   a successful result is detected, or 'ALL' to print summary      */
/*   information always. Default is 'ALL'.                     */
/*                                                   */
/*******************************************************************/
stOutDSname = 'output-dataset'
printStatus = 'ALL'
printSummary = 'ALL'
```

REXX Configuration, Part 4 of 4

```
/********************************************************************************/
/*                                                              */
/* SVC log settings                                             */
/*                                                              */
/* Instructions:                                                */
/* Change 'svc-log-dataset' to the name of the data set to which you */
/*   would like to send run SVCs log information.              */
/*                                                              */
/********************************************************************************/
svcLogDSname       = 'svc-log-dataset'
svcLogDSlrec       = '133'
svcLogDSblksz      = '1330'
svcLogDSpriSp      = '5'
svcLogDSsecSp      = ‘1’

/********************************************************************************/
/*                                                              */
/* PC log settings                                              */
/*                                                              */
/* Instructions:                                                */
/* Change 'pc-log-dataset' to the name of the data set to which you  */
/*   would like to send run PCs log information.               */
/*                                                              */
/********************************************************************************/
pcLogDSname        = 'pc-log-dataset'
pcLogDSlrec        = '133'
pcLogDSblksz       = '1330'
pcLogDSpriSp       = '100'
pcLogDSsecSp       = '40'
```

The Started Task

```
//BPNZACS PROC
/*********************************************************************/
/* THIS EXECUTES THE BPNZACS PROGRAM FOR INTEGRITY TESTING.          */
/* PUT THIS JCL IN THE PROCLIB DATA SET USED FOR STARTED TASKS       */
/* AND MAKE THE CORRESPONDING RACF UPDATES, E.G.                     */
/*   RDEFINE STARTED BPNZACS.** UACC(NONE) STDATA(USER(user)         */
/*     GROUP(SYS1) TRUSTED(YES))                                     */
/*   SETR RACLIST(STARTED) REFRESH                                   */
/*                                                                   */
/* INSTRUCTIONS:                                                     */
/*   CHANGE loadlib-dataset TO THE LOAD LIB DATASET UNDER YOUR HLQ   */
/*   CHANGE output-dataset TO THE ALLOCATED DATASET SPECIFIED FOR    */
/*     OUTPUT                                                        */
/*********************************************************************/
//GOSTEP EXEC PGM=BPNGMAIN,TIME=NOLIMIT
//STEPLIB  DD DSN=loadlib-dataset,DISP=SHR
//MYOUTDD  DD DSN=output-dataset,DISP=SHR
```

Generating the PC Table

```
//ZACSJP JOB NOTIFY=&SYSUID,MSGCLASS=A,REGION=5M
//*****************************************************************
//* GENERATES THE PC TABLE FOR INTEGRITY TESTING.                 *
//*                                                               *
//* INSTRUCTIONS:                                                 *
//*   CHANGE loadlib-dataset TO THE LOAD LIB DATASET UNDER YOUR HLQ   *
//*****************************************************************
//DELETE   EXEC PGM=IEFBR14
//DELDSN   DD DISP=(MOD,DELETE),DSN=&SYSUID..ZACS.PCNUM,
//            SPACE=(TRK,1),UNIT=SYSDA
//*
//CREATE   EXEC PGM=BPNGPCN
//STEPLIB  DD DSN=loadlib-dataset,DISP=SHR
//BPNPCOUT DD DISP=(NEW,CATLG),DSN=&SYSUID..ZACS.PCNUM,
//            SPACE=(TRK,(10,10)),UNIT=SYSDA,
//            DCB=(LRECL=133,BLKSIZE=0,RECFM=FBA)
//SYSOUT   DD SYSOUT=*
//STDOUT   DD SYSOUT=*
//STDERR   DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

Generating the SVC Table

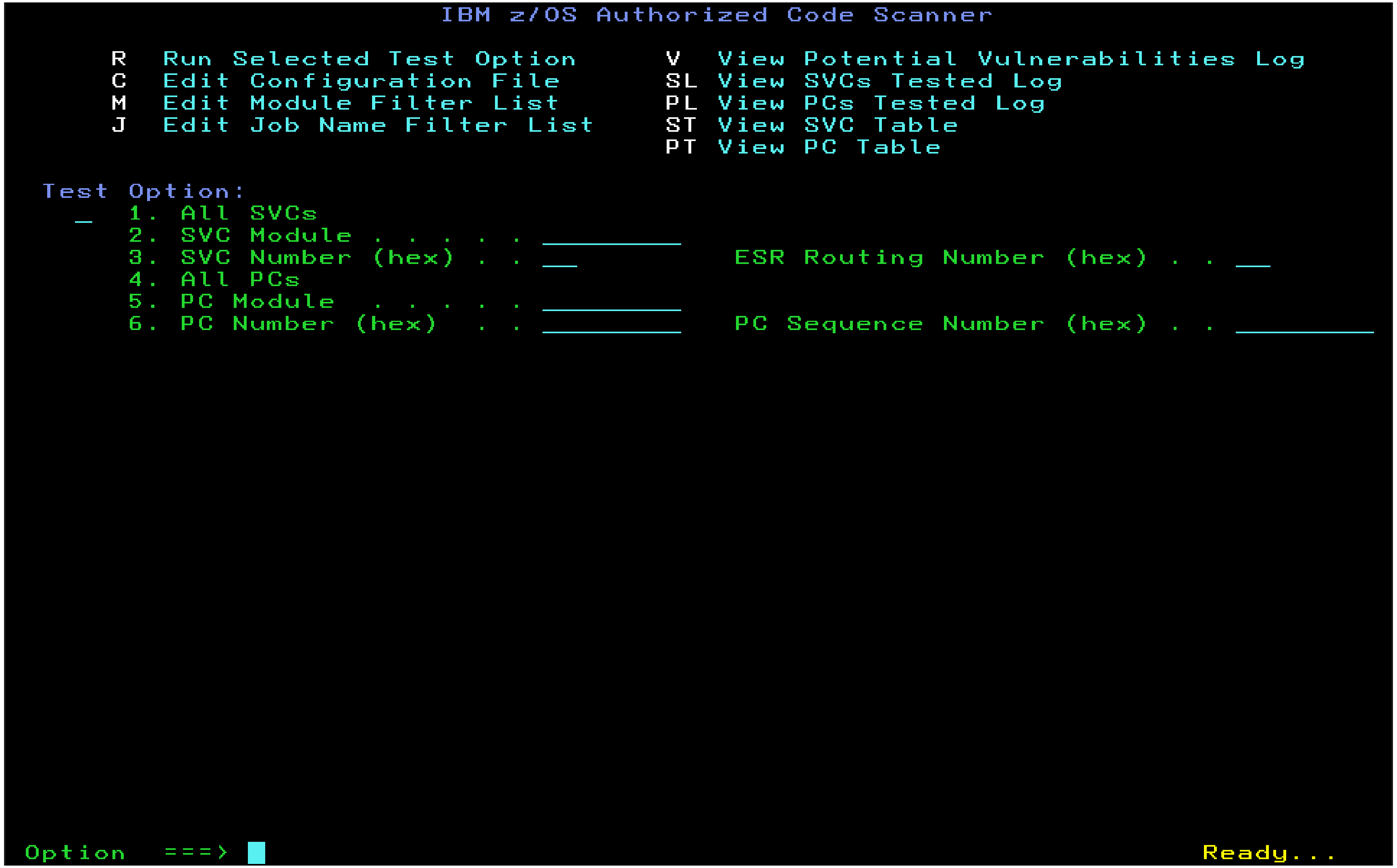
```
//ZACSJS JOB  NOTIFY=&SYSUID,MSGCLASS=A,REGION=5M
//*****************************************************************
//* GENERATES THE SVC TABLE FOR INTEGRITY TESTING.                *
//*                                                               *
//* INSTRUCTIONS:                                                 *
//*   CHANGE loadlib-dataset TO THE LOAD LIB DATASET UNDER YOUR HLQ   *
//*****************************************************************
//DELETE   EXEC PGM=IEFBR14
//DELDSN   DD DISP=(MOD,DELETE),DSN=&SYSUID..ZACS.SVCNUM,
//            SPACE=(TRK,1),UNIT=SYSDA
//*
//CREATE   EXEC PGM=BPNGSVCN
//STEPLIB  DD DSN=loadlib-dataset,DISP=SHR
//BPNSVOUT DD DISP=(NEW,CATLG),DSN=&SYSUID..ZACS.SVCNUM,
//            SPACE=(TRK,(10,10)),UNIT=SYSDA,
//            DCB=(LRECL=133,BLKSIZE=0,RECFM=FBA)
//SYSOUT   DD SYSOUT=*
//STDOUT   DD SYSOUT=*
//STDERR   DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

Secure Configuration

In addition to securing the load modules, the REXX, the started task and the associated input & output data sets, access to running the tool needs to be secured via the XFACILIT class with entity name BPN.RUN…

1. SETR CLASSACT(XFACILIT) RACLIST(XFACILIT)
2. RDEFINE XFACILIT BPN.RUN UACC(NONE) AUDIT(ALL)
3. PERMIT BPN.RUN CLASS(XFACILIT) ID(user or group ID) ACCESS(READ)
4. SETR RACLIST(XFACILIT) REFRESH

ISPF Support



```
                          IBM z/OS Authorized Code Scanner

      R   Run Selected Test Option      V   View Potential Vulnerabilities Log
      C   Edit Configuration File       SL  View SVCs Tested Log
      M   Edit Module Filter List       PL  View PCs Tested Log
      J   Edit Job Name Filter List     ST  View SVC Table
                                        PT  View PC Table

  Test Option:
   _     1. All SVCs
         2. SVC Module . . . . . . ________
         3. SVC Number (hex) . . __         ESR Routing Number (hex) . . __
         4. All PCs
         5. PC Module  . . . . . . ________
         6. PC Number (hex)   . . ________   PC Sequence Number (hex) . . ________

 Option   ===>                                                      Ready...
```

Highlights:

- Configuration
- Filters
- Inputs
- Outputs

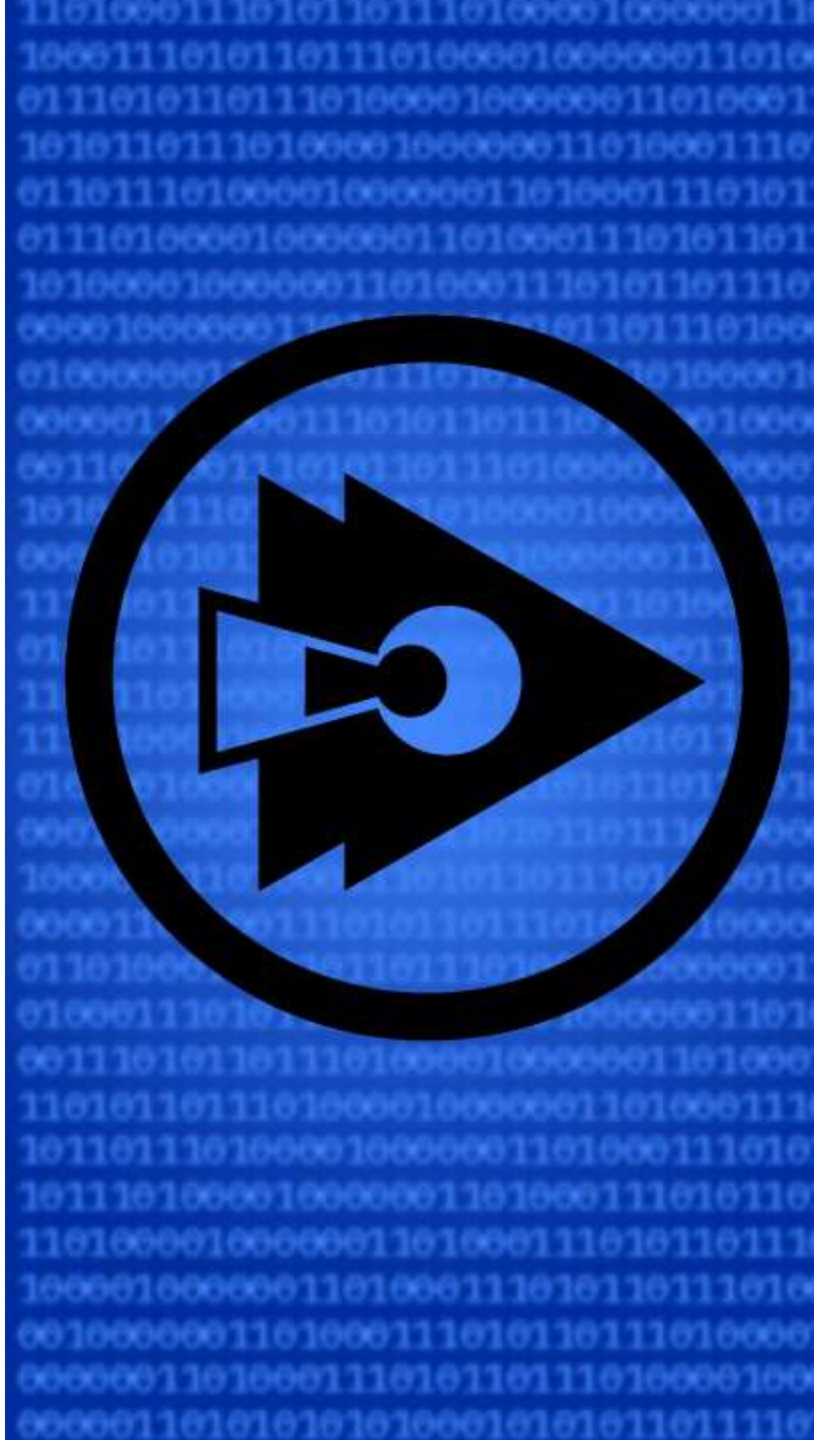
Turning the Feature On

The **IBM z/OS Authorized Code Scanner (zACS)** dynamically scans the client’s authorized code and provides diagnostic information for subsequent investigation as needed. Upon purchase, it is activated via IFAPRDxx in parmlib:

for subsequent investigation as needed. Upon purchase, it is activated via IFAPRDxx in parmlib:

```
PRODUCT OWNER('IBM CORP’)
NAME('z/OS’)
ID(5650-ZOS)
VERSION(*)
RELEASE(*)
MOD(*)
FEATURENAME('ZACS’)
STATE(ENABLED)
```

Documentation can be found here: www.ibm.biz/zacskc2020



Thank You

Questions?