z/OS 3.1 IBM Education Assistant

Solution Name: z/OS Authorized Code Monitor (zACM)

Solution Element(s): IBM z/OS Authorized Code Scanner

July 2023

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives

- New monitor that is safe to run on production systems

Overview

- Who (Audience)
  - Customers looking to mitigate the risk of integrity issues on their systems
- What (Solution)
  - New real-time monitoring capabilities
- Wow (Benefit / Value, Need Addressed)
  - The monitor is non-disruptive, allowing it to be safely used on production systems

Usage & Invocation

- Started task
  - Optional Parm – Set the BPNZ slip for first failure data capture
    - Takes a dump when a zACM hit occurs, without needing to set the generated sample slip
    - Syntax: PARM=(Matchlim, Description)
      - Matchlim to be added to the BPNZ Slip, up to 99
      - Description to be added to the BPNZ SLIP trap
  - Option Filter DDs
    - Include or exclude based on module name or job name
      - Only include *or* exclude may be specified at one time
    - Filter types:
      - MYMODIN - Include module names
      - MYMODEX - Exclude module names
      - MYJOBIN - Include job names
      - MYJOBEX - Exclude job names

```
//BPNZACM PROC
//GOSTEP EXEC PGM=BPNHMAIN,TIME=NOLIMIT,
//            PARM=(10,MY-DESCRIPTION)
//MYOUTDD  DD DSN=ZACM.TEST.OUTPUT,DISP=SHR
//MYSUMDD  DD DSN=ZACM.TEST.OUT.SUM,DISP=SHR
//MYMODIN  DD DSN=ZACM.INCL.MOD,DISP=SHR
//*MYMODEX  DD DSN=ZACM.EXCL.MOD,DISP=SHR
//*MYJOBIN  DD DSN=ZACM.INCL.JOB,DISP=SHR
//*MYJOBEX  DD DSN=ZACM.EXCL.JOB,DISP=SHR
```

- SMF record 1154 subtype 84 can be used to verify zACM is running for ZSCC compliance
- Once zACM is running, periodically check the output data set to check for a hit
  - Dumps produced from first failure data capture, if enabled, also indicate a hit
  - Output and summary data sets cleared upon restart

Interactions & Dependencies

- Software Dependencies
  - Running 2.4 or greater
- Hardware Dependencies
  - N/A
- Exploiters
  - N/A

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- Dependency on OA61444, OA61443, OA61760, OA60659, OA62619, PH45491

Installation & Configuration

- Due to its sensitive nature, all datasets containing the tool and its output must be protected
- Define a new profile for BPNZACM:

```
RDEFINE STARTED BPNZACM.** UACC(NONE) STDATA(USER(user)
GROUP(SYS1) TRUSTED(YES))
```

- Same registration as the IBM z/OS Authorized Code Scanner

```
PRODUCT OWNER('IBM CORP')
NAME('z/OS')
ID(5655-ZOS)
VERSION(*) RELEASE(*) MOD(*)
FEATURENAME('ZACS')
STATE(ENABLED)
```

- Data sets containing zACM (SYS1.BPN.SBPNLPA by default) must be added to LPALIB

Summary

- The monitor captures similar potential vulnerabilities to the scanner, but does so passively
- The monitor can be used on production systems
- First failure data capture, configured on the started task can be used to get dumps when the hit first occurs
  - Monitor events are triggered by normal activity on the system and may not be easily reproduceable

Appendix

- Publication
  - IBM z/OS Authorized Code Scanner Guide