IBM Education Assistance

Solution (Epic) Name: JES2 Exploitation of Non-Executable Memory

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Trademarks

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

Session Objectives

- Briefly introduce the Instruction Execution Protection (IEP) service that is provided by the z14 hardware.
- Describe changes made in JES2 to take advantage of this service

Overview

- Who (Audience)
  - Anyone and everyone who uses or abuses JES2 on z/OS 2.4 will be impacted.
- What (Solution)
  - We are moving as much data as we can into non-executable storage with the IEP service.
- Wow (Benefit / Value, Need Addressed)
  - By utilizing the IEP service we can significantly reduce the target size of JES2 for stack overflow and other similar attacks.
  - This can also help protect important data from poorly written programs.

Usage & Invocation Part 1

- What is this Instruction Execution Protection (IEP) service?
  - Well, it's exactly what it sounds like.
  - IEP is a service provided by the z14 hardware that allows us to get storage in a non-executable state.
  - When code attempts to run inside storage allocated with this service an ABEND occurs (0C4).
- Using the IEP service is pretty straight forward.
  - First, you upgrade to the proper hardware and software.
  - After that it is all automatic. JES2 will continue to work as usual except that more data will be put into non-executable storage.

Usage & Invocation Part 2

- Using the IEP service in your own JES2 exit code is relatively easy too.
  - You simply add EXECUTABLE=YES to your calls to $GETMAIN when you are getting storage for executable code. Otherwise, you ignore the EXECUTABLE= option.
    - The EXECUTABLE= keyword was added to $GETMAIN in z/OS 2.3
  - The default setting for $GETMAIN is now EXECUTABLE=NO.
    - The default in 2.3 was EXECUTABLE=YES.
  - If you specify EXECUTABLE= as a non default value you will need to specify the same value on the corresponding $FREMAIN call.

Usage & Invocation Part 2b

- Examples:

```
$GETMAIN RC,
      LV=(R2),
      SP=$ENFPPOL,
      KEY=1,
      LOC=ANY,
      EXECUTABLE=YES,
      ZEROSTOR=YES
```

This is a **non-default** call to $GETMAIN

```
$FREMAIN R,LV=(R0),A=R1,
      EXECUTABLE=YES
```

This is a **non-default** call to $FREMAIN.

```
$GETMAIN RC,
      LV=(R2),
      SP=$ENFPPOL,
      KEY=1,
      LOC=ANY,
      ZEROSTOR=YES
```

This is a default call to $GETMAIN

```
$FREMAIN R,LV=(R0),A=R1
```

This is a default call to $FREMAIN.

Interactions & Dependencies

- To exploit this item, all systems in the Plex must be at the new z/OS level: No, it is supported on each system of the plex
- Software Dependencies
  - EXECUTABLE=YES is only valid for sub pools 0-127, 129-132, 229-230, 236-237, 240, 244, and 249-252.
  - It is ignored for all other sub pools.
- Hardware Dependencies
  - Must be running on z14 or newer hardware.
- Exploiters
  - JES2 and any exit using the JES2 $GETMAIN macro.

Migration & Coexistence Considerations

- The main consideration here is user or vendor written exit code.
- The change to the default behavior of $GETMAIN has a chance to alter the behavior of any program that uses it.
  - However, we estimate the risk of disruption to be quite low.

Installation

- Nothing special required.

Session Summary

- In this session we discussed what IEP is plus the how and why JES2 is using it.
  - IEP is a service provided by the z14 hardware that allows storage to be allocated in a read only or non-executable state.
  - JES2 is taking advantage of this service by changing the default behavior of our $GETMAIN macro.
    - Additional uses of this service are planned for future updates and releases.
  - JES2 is using this service to reduce its attack surface to stack overflow type attacks and to protect data from poorly written programs.

Appendix

- IBM z14 Technical Introduction.
- IBM z14 (3906) Technical Guide.
- IBM Knowledge Center: Migrate to an IBM z14 server(https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.e0zm100/z14.htm)
- z/OS V2R4.0 JES2 Macros – SA32-0996-40