**堆溢出检测**

1.1 SARD-testsuite-6/testcaseid=1572

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

失败

1. 原因分析：

由整数溢出导致的堆溢出，微执行设置设置malloc参数是一个符号值，默认求解所得的是一个超大的数，并不会溢出。

1. 改进

无

1.2 SARD-testsuite-6/testcaseid=1573

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

失败

1. 原因分析：

由整数溢出导致的堆溢出，微执行设置设置malloc参数是一个符号值，默认求解所得的是一个超大的数，并不会溢出。

1. 改进

无

1.3 SARD-testsuite-6/testcaseid=1573

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

正常

3)原因分析：

无

4)改进

无

1.4 SARD-testsuite-6/testcaseid=1575

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

由整数溢出导致的堆溢出，微执行设置设置malloc参数是一个符号值，默认求解所得的是一个超大的数，并不会溢出。

4)改进

无

1.5 SARD-testsuite-6/testcaseid=1576

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

正常

1. 原因分析：

无

1. 改进

无

1.6 SARD-testsuite-6/testcaseid=1577

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

由整数溢出导致的堆溢出，微执行设置设置malloc参数是一个符号值，默认求解所得的是一个超大的数，并不会溢出。

4)改进

无

1.7 SARD-testsuite-6/testcaseid=1577

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

正常

3)原因分析：

无

4)改进

无

1.8 SARD-testsuite-6/testcaseid=1611

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

程序运行异常

3)原因分析：

angr内部异常

4)改进

等待官方修复

1.9 SARD-testsuite-6/testcaseid=1612

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

程序运行异常

3)原因分析：

angr内部异常

4)改进

等待官方修复

1.10 SARD-testsuite-6/testcaseid=1614

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

strcpy拷贝当中，由于源字符串过长可能导致溢出，但angr微执行过程中，会将构造的符号化源字符串变为1，顾不会造成溢出。

4)改进

无

1.11 SARD-testsuite-6/testcaseid=1615

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

正常

3)原因分析：

无

4)改进

无

1.12 SARD-testsuite-6/testcaseid=1628

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

程序运行异常

3)原因分析：

strcpy拷贝当中，由于源字符串过长可能导致溢出，但angr微执行过程中，会将构造的符号化源字符串变为1，顾不会造成溢出。

4)改进

无

1.13 SARD-testsuite-6/testcaseid=1630

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

缺少对漏洞函数snprintf建模

4)改进

等待官方修复

1.14 SARD-testsuite-6/testcaseid=1631

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

正常

3)原因分析：

无

4)改进

无

1.15 SARD-testsuite-6/testcaseid=1632

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

缺少对漏洞函数snprintf建模

4)改进

等待官方修复

1.16 SARD-testsuite-6/testcaseid=1633

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

正常

3)原因分析：

无

4)改进

无

1.17 SARD-testsuite-6/testcaseid=1634

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

失败

3)原因分析：

缺少对漏洞函数snprintf建模

4)改进

等待官方修复

1.18 SARD-testsuite-6/testcaseid=1635

1)CWE编号

CWE-122: Heap-based Buffer Overflow

2)检测结果:

正常

3)原因分析：

无

4)改进

无