

Сценарии использования статического анализатора

Валерий Игнатьев

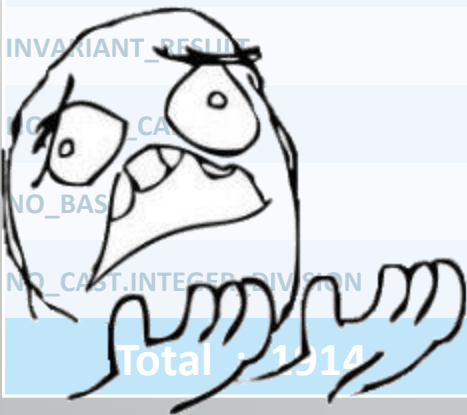
ИСП РАН

Типичное первое использование

Warning	#	Warning	#	Warning	#
BAD_COPY_PASTE	2	NO_CAST.INTEGER_OVERFLOW	95	NRE.RET.USER.PROC	3
CAST_AFTER_CHECK	1	NO_LOCK.STAT	107	NRE.RET.USER.PROC.ARGUMENT	3
HANDLE_LEAK	78	NRE	7	NRE.RET.USER.PROC.STATISTICAL	30
HANDLE_LEAK.EXCEPTION	401	NRE.ARGUMENT	20	SIMILAR_BRANCHES	20
HANDLE_LEAK.EXCEPTION.Dispose	251	NRE.DEREF_AFTER_AS	4	UNREACHABLE_CODE	94
HANDLE_LEAK.EXCEPTION.WriteLine	79	NRE.DEREF_AFTER_AS.INSTANT	1	UNREACHABLE_CODE.EXCEPTION	9
INFINITE_LOOP	1	NRE.DEREF_AFTER_NULL	18	UNREACHABLE_CODE.SYNTAX	3
INVARIANT_RESULT	578	NRE.DEREF_AFTER_NULL.ARGUMENT	3	UNUSED_VALUE	22
NO_BASE_CALL.LIB	8	NRE.NULL_AFTER_DEREF	27	WRONG_ARGUMENTS_ORDER	1
NO_BASE_CALL.STAT	6	NRE.RET.LIB.PROC.Container.STATISTICAL	6	WRONG_SEMICOLON	1
NO_CAST.INTEGER_DIVISION	25	NRE.RET.LIB.PROC.STATISTICAL	10		
Total : 1914					

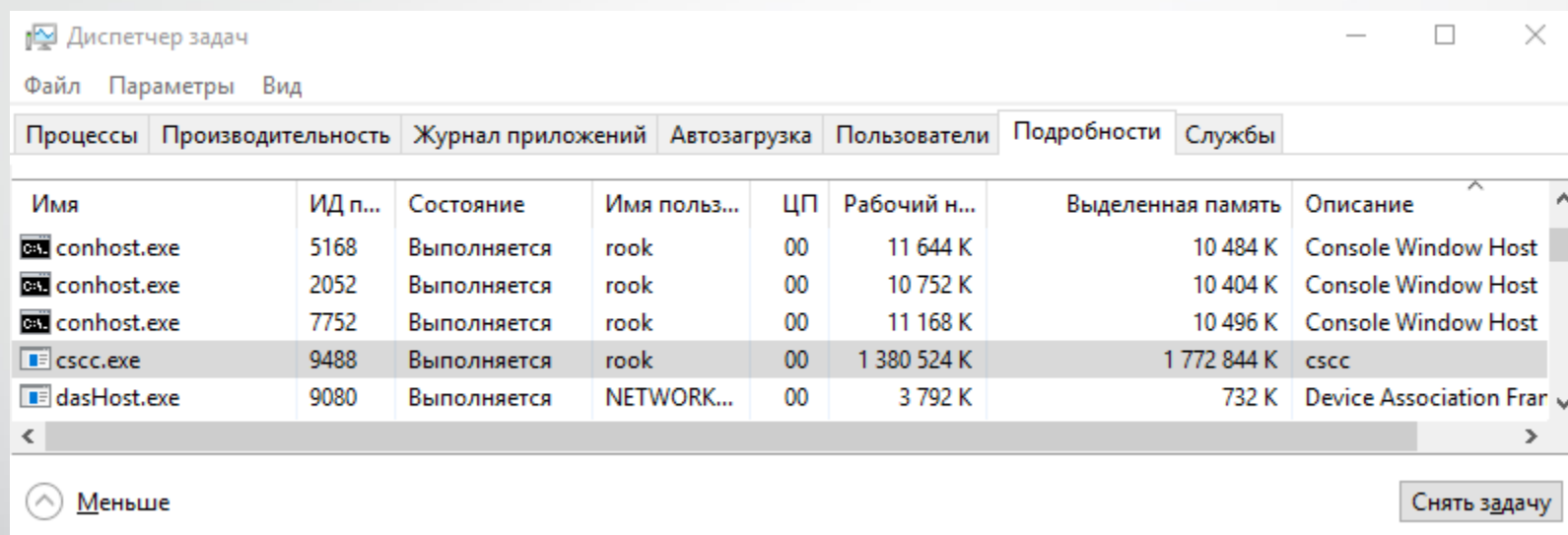
Типичное первое использование

Warning	#	Warning	#	Warning	#
BAD_COPY_PASTE	2	NO_CAST.INTEGER_OVERFLOW	95	NRE.RET.USER.PROC	3
CAST_AFTER_CHECK	1	NO_LOCK.STAT	107	NRE.RET.USER.PROC.ARGUMENT	3
HANDLE_LEAK	78	NRE	7	NRE.RET.USER.PROC.STATISTICAL	30
HANDLE_LEAK.EXCEPTION	401	NRE.ARGUMENT	20	SIMILAR_BRANCHES	20
HANDLE_LEAK.EXCEPTION.Dispose	251	NRE.DEREF_AFTER_AS	4	UNREACHABLE_CODE	94
HANDLE_LEAK.EXCEPTION.WriteLine	79	NRE.DEREF_AFTER_AS.INSTANT	1	UNREACHABLE_CODE.EXCEPTION	9
INFINITE_LOOP	1	NRE.DEREF_AFTER_NULL	18	UNREACHABLE_CODE.SYNTAX	3
INVARIANT_RESULT	578	NRE.DEREF_AFTER_NULL.ARGUMENT	3	UNUSED_VALUE	22
NO_CAST.INTEGER_OVERFLOW	8	NRE.NULL_AFTER_DEREF	27	WRONG_ARGUMENTS_ORDER	1
NO_BASED_CAST	6	NRE.RET.LIB.PROC.Container.STATISTICAL	6	WRONG_SEMICOLON	1
NO_CAST.INTEGER.DIVISION	25	NRE.RET.LIB.PROC.STATISTICAL	10		
Total 1514					



Исправление конкретной ошибки

Дано: Ненормально высокое потребление памяти



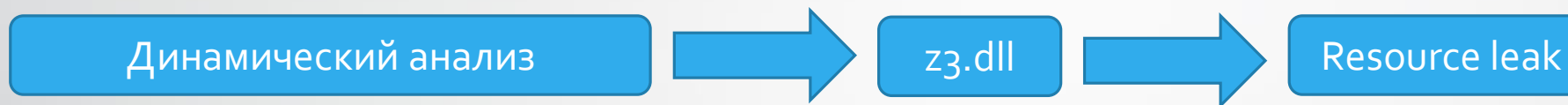
The screenshot shows the Windows Task Manager window titled "Диспетчер задач". The "Процессы" (Processes) tab is selected. The table lists several processes, with "cscc.exe" highlighted in blue, indicating it is the process of interest due to its high memory usage.

Имя	ИД п...	Состояние	Имя польз...	ЦП	Рабочий н...	Выделенная память	Описание
conhost.exe	5168	Выполняется	rook	00	11 644 K	10 484 K	Console Window Host
conhost.exe	2052	Выполняется	rook	00	10 752 K	10 404 K	Console Window Host
conhost.exe	7752	Выполняется	rook	00	11 168 K	10 496 K	Console Window Host
cscc.exe	9488	Выполняется	rook	00	1 380 524 K	1 772 844 K	cscc
dasHost.exe	9080	Выполняется	NETWORK...	00	3 792 K	732 K	Device Association Frar

```
[6607/17731] Completed  
Lucene.Net.Search.TopFieldCollector.MultiComparatorScoringMaxScoreCollector.MultiComparatorScoringMaxScoreCollector(Luce  
ne.Net.Search.FieldValueHitQueue<Lucene.Net.Search.FieldValueHitQueue.Entry>, int, bool) analyze time: 10 ms 48950 reqs,  
45931 SAT, 2942 UNSAT
```

Исправление конкретной ошибки

Дано: Ненормально высокое потребление памяти



Исправление конкретной ошибки

Дано: Ненормально высокое потребление памяти



Z3.Context,
Z3.BitVecExpr, Z3Object

```

399 public static int StoreCondition(ValueNumbering vn, params ICondition[] conds)
400 {
401     try
402     {
403         var vm = new VariableManager();
404         IList<ICondition> addedConditions;
405         var slv = SMTSolver.CreateAndFillBoolExprs(vn, conds, out addedConditions);
406         var request = vm.Ctx.BenchmarkToSMTString("test", "QF_UFBV", "unknown", "", slv.ToArray(),
407             vm.Ctx.MkTrue());
408         var reqBytes = _encoding.GetBytes(request);
409         var length = _encoding.GetByteCount(request);
410         lock (FilePath)
411         {
412             if (_stream == null)
413             {
414                 _stream = new FileStream(FilePath, FileMode.OpenOrCreate);
415             }
416             _positionsAndSizes.Add(new Tuple<long, int>(_stream.Position, length));
417             _stream.Write(reqBytes, 0, length);
418
419             return Count++;
420         }
421     }
422     catch (Exception e)
423     {
424         Log.ErrorException("Can't store SMT request", e);
425         return -1;
426     }
427 }

```

8 %

CSCC Analysis Tool

analyze Initialize Finished. 243 warnings found

han

HANDLE_LEAK: vm is not disposed at the end of the function

C:\cygwin\home\rook\src\CSharpCodeChecker\AnalyzersAndCodeFixes\DiagnosticAnalyzers\Analysis\SMTSolver.cs 426:8

created

C:\cygwin\home\rook\src\CSharpCodeChecker\AnalyzersAndCodeFixes\DiagnosticAnalyzers\Analysis\SMTSolver.cs 403:26

assigned

C:\cygwin\home\rook\src\CSharpCodeChecker\AnalyzersAndCodeFixes\DiagnosticAnalyzers\Analysis\SMTSolver.cs 403:21

return

C:\cygwin\home\rook\src\CSharpCodeChecker\AnalyzersAndCodeFixes\DiagnosticAnalyzers\Analysis\SMTSolver.cs 419:21

HANDLE_LEAK: new AdhocWorkpage() is not disposed at the end of the function

CSCC Analysis Tool

.NET Reflector Analy...

NuGet browser

Find Results

Список ошибок

Вывод

Результаты поиска 1

Точки останова

Параметры

Стабилизация перед релизом

Цель: исправить максимальное число наиболее критических ошибок в кратчайшие сроки

Предупреждения	Предыдущий релиз	Будущий релиз	Исчезло	Новые
Всего	1000	1100	150	250
NRE	150	170	15	35
UNREACHABLE	100	110	15	25
RESOURCE_LEAK	10	15	1	6
UNUSED_VALUE	500	600	0	100
...

Стабилизация перед релизом

Цель: исправить максимальное число наиболее критических ошибок в кратчайшие сроки

Предупреждения	Предыдущий релиз	Будущий релиз	Исчезло	Новые
Всего	1000	1100	150	250
NRE	150	170	15	35
UNREACHABLE	100	110	15	25
RESOURCE_LEAK	10	15	1	6
UNUSED_VALUE	500	600	0	100
...

- Важную роль играет не просто обнаружение ошибки, но и указание условий, при которых она может проявиться

TestStressIndexing2.cs TestMixedCodecs.cs QueryRescorer.cs BlockTreeTermsReader.cs

C# Lucene.Net Lucene.Net.Search.QueryRescorer Rescore(IndexSearcher searcher, Top

```
68     Scorer scorer = null;
69
70     while (hitUpto < hits.Length)
71   {
72       ScoreDoc hit = hits[hitUpto];
73       int docID = hit.Doc;
74       AtomicReaderContext readerContext = null;
75       while (docID >= endDoc)
76       {
77           readerUpto++;
78           readerContext = leaves[readerUpto];
79           endDoc = readerContext.DocBase + readerContext.Reader.MaxDoc;
80       }
81
82       if (readerContext != null)
83       {
84           // We advanced to another segment:
85           docBase = readerContext.DocBase;
86           scorer = weight.Scorer(readerContext, null);
87       }
88
89       int targetDoc = docID - docBase;
90       int actualDoc = scorer.DocID();
```

98 %

CSCC Analysis Tool

Analyze Initialize Finished. 1423 warnings found nre Show

D:\CSharpCodeCheckerTests\lucenenet\src\Lucene.Net.Tests\Core\Index\TestStressIndexing2.cs 412:42

NRE: Value scorer, which has null value, is dereferenced in method call scorer.DocID()

D:\CSharpCodeCheckerTests\lucenenet\src\Lucene.Net.Core\Search\QueryRescorer.cs 89:32

declared at

D:\CSharpCodeCheckerTests\lucenenet\src\Lucene.Net.Core\Search\QueryRescorer.cs 68:20

Step 1: Condition hitUpto < hits.Length taking true branch.

D:\CSharpCodeCheckerTests\lucenenet\src\Lucene.Net.Core\Search\QueryRescorer.cs 70:13

Step 2: Condition docID >= endDoc taking false branch.

D:\CSharpCodeCheckerTests\lucenenet\src\Lucene.Net.Core\Search\QueryRescorer.cs 75:17

Step 3: Condition readerContext != null taking false branch.

D:\CSharpCodeCheckerTests\lucenenet\src\Lucene.Net.Core\Search\QueryRescorer.cs 82:17

NIDE ADJUSTMENT: Value null is dereferenced inside function CheckScore()

CSCC Analy... .NET Reflect... NuGet brow... Find Results Список ош... Вывод Результаты... Точки остан... Параметр

Регулярный анализ

- ✓ Повышение качества ПО
- ✓ Снижение средней стоимости исправления ошибки
- ✓ Возможность постоянного контроля стабильности
- ✓ Интеграция в процесс разработки (проверка коммитов, ночных сборок)
- ✓ Интеграция с Code Review
- ✓ Облегчение поиска сложно воспроизводимых ошибок

Коммерческие инструменты



Coverity



Klocwork



ISP RAS



PVS-Studio

Контактная информация

- Валерий Игнатъев (rook@ispras.ru)
- Владимир Кошелев (vedun@ispras.ru)
- Артем Борзилов (helendile@ispras.ru)
- <http://sharpchecker.ispras.ru>