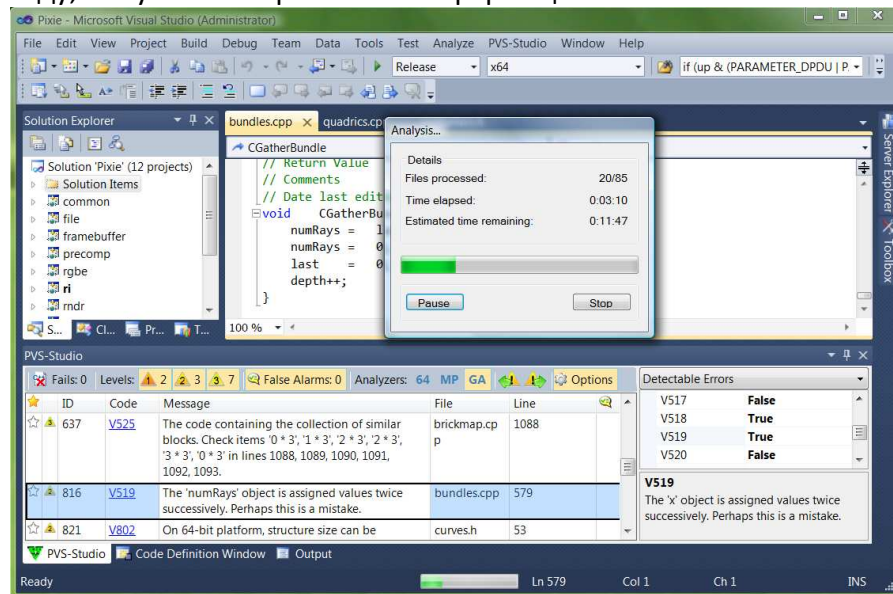


PVS-Studio - статический анализатор, выявляющий ошибки в исходном коде приложений на языке C/C++/C++0x. Можно выделить 3 набора правил, включенных в состав PVS-Studio:

1. Диагностика 64-битных ошибок (Viva64)
2. Диагностика параллельных ошибок (VivaMP)
3. Диагностика общего назначения

Инструмент PVS-Studio предназначен для разработчиков современных приложений и интегрируется в среду Visual Studio 2005/2008/2010. При этом предоставляется удобный пользовательский интерфейс для анализа файлов, навигации по коду, получению справочной информации.



Работа с анализатором не требует предварительного изучения документации и настройки. Анализатор готов к работе сразу же после инсталляции.

Особенности PVS-Studio

- интеграция с Visual Studio 2005/2008/2010;
- поддержка систем непрерывной интеграции;
- online-справка на русском и английском языке;
- документация в pdf;
- сохранение и загрузка результатов анализа;
- работа на всех ядрах и процессорах;
- лидер в диагностике 64-битных ошибок;
- оценка сложности 64-битной миграции кода;
- интерактивные фильтры;
- удобная интеграция в командный процесс разработки;
- разметка текста программы для проверки только нового кода.

Достаточно общих слов. Нет рекламным текстам! Намного лучше о возможностях PVS-Studio расскажут примеры. Вот, что находит наш анализатор кода в некоторых приложениях.



Return to Castle Wolfenstein - компьютерная игра, шутер от первого лица, разработанный компанией id Software.

V564 The '&' operator is applied to bool type value. You've probably forgotten to include parentheses or intended to use the '&&' operator. g_client.c 1534

```
#define SVF_CASTAI 0x00000010
if (!ent->r.svFlags & SVF_CASTAI)
```

Забывты скобки. Вначале вычисляется подвыражение "!ent->r.svFlags", а уже затем выполняется операция '&'.



Miranda IM - программа мгновенного обмена сообщениями.

V567 Undefined behavior. The 's' variable is modified while being used twice between sequence points. ezxml.c 371

```
while (*(n = ++s + strspn(s, EZXML_WS)) && *n != '>') {
```

Нет гарантии, что 's' будет увеличена перед вызовом функции strspn().



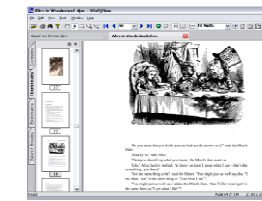
Chromium - веб-браузер с открытым исходным кодом, разработанный компанией Google. На основе Chromium создаётся браузер Google Chrome.

V554 Incorrect use of auto_ptr. The memory allocated with 'new []' will be cleaned using 'delete'. accessibility_win_browsertest.cc 171

```
auto_ptr<VARIANT> child_array(new VARIANT[child_count]);
```

Использовать auto_ptr для массивов нельзя. В деструкторе auto_ptr уничтожается только один элемент:

```
~auto_ptr() { delete _MyPtr; }
```



WinDjView - быстрая и компактная программа для просмотра файлов формата DjVu.

V560 A part of conditional expression is always true: 0xA. xmlparser.cpp 45

```
inline bool IsValidChar(int c) {
    return c == 0x9 || 0xA || c == 0xD || c >= 0x20 && c <= 0xD7FF
        || c >= 0xE000 && c <= 0xFFFFD
        || c >= 0x10000 && c <= 0x10FFFF;
}
```

Опечатались и случайно написали "0xA" вместо "c == 0xA".



FCE Ultra – открытый эмулятор приставки Nintendo Entertainment System.

V561 It's probably better to assign value to 'x' variable than to declare it anew. Previous declaration: ines.cpp, line 960. ines.cpp 962

```
fp = fopen(name, "wb");
int x = 0;
if (!fp)
    int x = 1;
```

Лишний раз объявили переменную 'x'. В результате эмулятор всегда считает, что ему удалось открыть файл.



TortoiseSVN

TortoiseSVN — клиент для системы контроля версий Subversion.

V547 Expression '* utf8CheckBuf == 0xC0' is always false. The value range of signed char type: [-128, 127]. tortoiseblame.cpp 310 (и ещё два предупреждения V547)

```
// check each line for illegal utf8 sequences.
char * utf8CheckBuf = lineptr;
while ((bUTF8)&&(*utf8CheckBuf)) {
    if ((*utf8CheckBuf == 0xC0) ||
        (*utf8CheckBuf == 0xC1) ||
        (*utf8CheckBuf >= 0xF5)) {
```

Не проверяем то, что хотели. Выражение всегда ложно.



WinMerge — свободное ПО с открытым исходным кодом для сравнения и синхронизации файлов и директорий.

V530 The return value of function 'empty' is required to be utilized. DirActions.cpp 1307, 1308

```
if (diffpos == (UINT_PTR)SPECIAL_ITEM_POS)
{
    strLeft.empty();
    strRight.empty();
}
```

При определенном условии код должен очистить строки. Но вместо `std::string::clear()`, случайно написали `std::string::empty()`.



Notepad++ - свободный текстовый редактор с подсветкой синтаксиса.

V512: A call of the memset function will lead to a buffer overflow or underflow. DockingManager.cpp 60

```
#define CONT_MAP_MAX 50
int _iContMap[CONT_MAP_MAX];
...
memset(_iContMap, -1, CONT_MAP_MAX);
```

Заполнили только часть массива, так как забыли умножить "CONT_MAP_MAX" на "sizeof(int)".



Newton Game Dynamics - популярный физический движок для симуляции физического поведения объектов окружающей среды.

V502 Perhaps the '?' operator works in a different way than it was expected. The '?' operator has a lower priority than the '*' operator. dgminkowskiconv.cpp 1061

```
den = dgFloat32(1.0e-24f) *
    (den > dgFloat32(0.0f)) ? dgFloat32(1.0f) : dgFloat32(-1.0f);
```

Приоритет оператора '?' ниже, чем у оператора умножения '*'.



Fennec Media Project - универсальный медиа-плеер.

V540 Member 'lpstrFilter' should point to string terminated by two 0 characters. windows.c 5309

```
OPENFILENAME lofn;
...
lofn.lpstrFilter = uni("All Files (*.*)\0*.*");
```

Забыли, что в конце должно быть два нуля. Здесь и юнит-тесты не помогут. Только ручное тестирование. Корректный вариант: `lofn.lpstrFilter = uni("All Files (*.*)\0*.*\0");`

Подробнее с инструментом PVS-Studio вы можете познакомиться на сайте: <http://www.viva64.com/ru/pvs-studio/>

Вы также можете скачать ознакомительную версию: <http://www.viva64.com/ru/pvs-studio-download/>

Контактная информация

ООО «СиПроВер»
Сайт: www.viva64.com
Электронная почта: support@viva64.com

Юридический адрес:
300027, г. Тула, ул. Металлургов, 70-1-88

Почтовый ящик:
300027, г. Тула, а/я 1800

Наш офис:
г. Тула, ул. Кутузова, 100, 7-й этаж, офис 73

Телефон: (4872) 38-59-95.
Мы работаем с 9:00 до 18:00 по московскому времени.



PVS-Studio
поиск ошибок в коде
C / C++ / C++0x

ООО «Системы программной верификации»

www.viva64.com