

СТАТИЧЕСКИЙ АНАЛИЗАТОР SVACE



Svace – необходимый инструмент жизненного цикла разработки безопасного ПО, основной статический анализатор компании Samsung. Обнаруживает более 50 классов критических ошибок в исходном коде. Поддерживает языки C, C++, C#, Java; Kotlin и Go – в предварительной версии. Включён в Единый реестр российского ПО (№4047).

ИСП РАН

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Svace – постоянно развивающийся инновационный продукт, основанный на многолетних исследованиях. Объединяет ключевые качества иностранных аналогов (Coverity Scan Static Analysis, Fortify Static Code Analyzer, Klocwork Static Code Analysis) с уникальным использованием открытых промышленных компиляторов в целях максимальной поддержки новых стандартов языков программирования.

SVACE – ЭТО:

- Высокое качество анализа:
 - точное представление исходного кода (благодаря интеграции с любой системой сборки);
 - полное покрытие всех путей с учетом связей между функциями для поиска сложных ошибок;
 - высокий процент истинных срабатываний (60-90%).
- Масштабируемость и высокая скорость:
 - параллельный анализ с использованием всех доступных процессорных ядер;
 - возможность анализировать системы из десятков

- миллионов строк кода (анализ Android 6 из 8 миллионов строк занимает 5-6 часов);
 - поддержка не только полного, но и инкрементального анализа системы (подразумевает быструю повторную проверку недавно измененного кода).
- Удобный интерфейс просмотра предупреждений:
 - подробное описание ошибок с навигацией по коду;
 - разделение срабатываний на истинные и ложные;
 - миграция результатов между запусками и сокрытие ложных срабатываний.
- Ускоренная кастомизация (конфигурация существующих детекторов, а также написание индивидуальных, доступных только данному заказчику; создание специфических интерфейсов);
- Ускоренная адаптация к работе с новым окружением (добавление новых компиляторов в течение 1-2 недель, в сложных случаях – до 2 месяцев);
- Полная совместимость с нормативными документами и требованиями регуляторов (ФСТЭК РФ).
- Возможность использования для реализации обеспечительных мер ГОСТ Р 56939-2016 (при необходимости сертификации ПО для использования на территории России), в том числе полная совместимость с новой «Методикой выявления уязвимостей и недеklarированных возможностей в программном обеспечении» ФСТЭК России (при необходимости сертификации ПО для использования на территории России).

ДЛЯ КОГО ПРЕДНАЗНАЧЕН SVACE?

- Компании, нацеленные на разработку ПО с высокой степенью надёжности и безопасности.
- Компании, которые нуждаются в сертификации разрабатываемого ПО.
- Испытательные лаборатории.

ОПЫТ ВНЕДРЕНИЯ

Svace – основной анализатор Samsung с 2015 года. Применяется для проверки собственного ПО компании на базе ОС Android и исходного кода ОС Tizen, которая используется в смартфонах, информационно-развлекательных системах и бытовой технике Samsung. С 2017 года Svace проверяет все изменения, присланные для рецензирования и включения в ОС Tizen. С 2020 года Svace применяется также в компании Huawei.

В России Svace используется более чем в 30 компаниях и лабораториях, в том числе в ОАО «РусБИТех», АО «Лаборатория Касперского», Postgres Professional, ООО «Код Безопасности», МВП «СВЕМЕЛ» и др.

ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ И АРХИТЕКТУРЫ

- Платформы, на которых работает анализатор: ОС на базе ядра Linux (начиная с версии 3.13), ОС Windows (начиная с Windows 7 SP 1) и WSL (версий 1 и 2).
- Архитектуры: Intel x86/x86-64, ARM/ARM64, MIPS/MIPS64, Power PC/Power PC 64, RISC-V 32/64, Hexagon (частично – AEON, TriCore, HIDSIP, OpenRISC для компилятора GCC).

ПОДДЕРЖИВАЕМЫЕ КОМПИЛЯТОРЫ

Для C/C++ (версий до C++17): GCC (GNU Compiler Collection), Clang (LLVM compiler), Microsoft Visual C++ Compiler, RealView/ARM Compilation Tools (ARMCC), Intel C++ Compiler, Wind River Diab Compiler, NEC/Renesas CA850, CC78K0(R) C Compilers, C/C++ Compiler for the Renesas M16C Series and R8C Family, Panasonic MN10300 Series C Compiler, C compiler for Toshiba TLCS-870 Family, Samsung CalmSHINE16 Compilation Tools, Texas Instruments TMS320C6* Optimizing Compiler и др.

Для C# (версий до C# 7): Roslyn, Mono.

Для Java (версий до Java 11): OpenJDK Javac Compiler, Eclipse ECJ compiler.

Для Kotlin: Kotlin 1.4.

Для Go: Go 1.14.

СХЕМА РАБОТЫ

