УДК 004.056

АНАЛИЗ МЕТОДОВ КЛАССИФИКАЦИИ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИХ ПРИМЕНЕНИЕ ПРИ ПРОВЕДЕНИИ СТАТИЧЕСКОГО АНАЛИЗА ИСХОДНОГО КОДА НА ЯЗЫКЕ ПРОГРАММИРОВАНИЯ JAVA

В.В. Семенов, М.Б. Довгаленко
(Санкт-Петербург, Университет ИТМО)
Научный руководитель – к.т.н. Гирик А.В.
(Санкт-Петербург, Университет ИТМО)

В настоящее время статический анализ исходного кода, т.е. анализ кода без его исполнения, является одним из наиболее эффективных способов автоматизации задачи обнаружения ошибок и уязвимостей уровня исходного кода. Разработано большое количество инструментов статического анализа, поддерживающих популярные языки программирования. Результатом работы таких инструментов обычно является формализованный отчет, чаще всего в формате XML. Однако эти инструменты не проводят четкой границы между уязвимостями и простыми ошибками. Кроме того, наиболее популярные инструменты статического анализа Java-кода, такие как Findbugs, SpotBugs, PVS-Studio, в отчетах об обнаруженных проблемах не предоставляют данных, пригодных для агрегированной оценки общей уязвимости программного обеспечения. В связи с этим возникает задача выбора такого способа классификации результатов, который позволил бы отличить простую ошибку от уязвимости и формально оценить влияние обнаруженной уязвимости на безопасность.

Целью работы является анализ методов классификации уязвимостей на предмет их применимости к ранжированию результатов выполнения статического анализа исходного кода.

Базовые положения исследования. В исследовании были уточнены понятия ошибки и уязвимости исходного кода, установлены критерии их отличия. Выявлено, что природа уязвимостей зависит от этапа жизненного цикла программного обеспечения. Область исследования ограничена уязвимостями этапа реализации и не затрагивает уязвимости, возникающие из-за неправильной конфигурации окружения, некорректных требований и т.д.

В ходе исследования был проведен обзор существующих методов классификации уязвимостей, выявлены те методы классификации, которые применимы для сравнительной оценки уязвимостей или могут быть доработаны для этих целей. Рассматривались иерархические, одномерные, многомерные и смешанные способы классификации.

В результате анализа было выявлено, что для решения поставленной задачи наиболее пригодны одномерные каталоги недочетов и уязвимостей, а также метод структурной классификации уязвимостей. Пример одномерного каталога – Common Weakness Enumeration (CWE). Существенный плюс CWE заключается в том, что в исследуемых анализаторах SpotBugs и PVS-Studio частично реализована данная классификация.

В структурном методе схема классификации описывается парами атрибут-значение вместо иерархической структуры. В такой модели каждый атрибут является свойством объекта. При этом объектом считается уязвимость, а свойствами могут быть те ошибки, которые приводят к уязвимости. Набор этих свойств идентифицирует конкретную уязвимость. Оказалось, что данный способ классификации помогает при ручном разборе уязвимостей и их первопричин, но плохо применим к автоматическому анализу.

В итоге по совокупности критериев был выбран способ классификации по каталогу CWE. Однако данный классификатор не дает численной оценки уязвимости. Таким образом,

с этой точки зрения выбранная система классификации нуждается в доработке, что является темой для дальнейших исследований.

На примере анализатора SpotBugs был проведен обзор доступных для обнаружения этим инструментом уязвимостей и составлена таблица соответствий кодов анализатора и каталога CWE. В рамках исследования таблица дополнена новыми соответствиями.

Результаты работы. Проведен анализ существующих методов классификации уязвимостей. Одномерный каталог CWE выбран в качестве метода классификации, наиболее соответствующего целям ранжирования результатов выполнения статического анализа исходного кода.