УДК 004.056

ИССЛЕДОВАНИЕ ОТКРЫТЫХ БАЗ УЯЗВИМОСТЕЙ И ОЦЕНКА ВОЗМОЖНОСТИ ИХ ПРИМЕНЕНИЯ В СИСТЕМАХ АНАЛИЗА ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

А. В. Федорченко[a], *младший научный сотрудник*
А. А. Чечулин[a], *канд. техн. наук, старший научный сотрудник*
И. В. Котенко[a], *доктор техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности*
[a]*Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, РФ*

Постановка проблемы: *ежегодно количество обнаруживаемых уязвимостей в программных и аппаратных продуктах остается на высоком уровне. Вместе с этим несогласованная работа компаний и организаций, занимающихся поиском и классификацией уязвимостей, приводит к уменьшению эффективности использования их баз уязвимостей в системах анализа защищенности. Целью работы является анализ открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей, в том числе получение статистики и выявление общих тенденций обнаружения уязвимостей в программно-аппаратном обеспечении.* ***Результаты:*** *проведены разбор и сравнение форматов открытых баз уязвимостей, таких как CVE, NVD, X-Force и OSVDB, а также форматов словарей продуктов и показателей, таких как CPE и CVSS, характеризующих уязвимости. Собрана статистика обнаруженных уязвимостей в распространенных операционных системах и веб-браузерах, получено распределение уязвимых продуктов основных разработчиков программного обеспечения за последние 10 лет. Выявлены общие тенденции обнаружения, опубликования и устранения уязвимостей в наиболее используемых продуктах различных производителей программного обеспечения (Microsoft, Google, Oracle, Apple и др.).* ***Практическая значимость:*** *анализ форматов представления уязвимостей в открытых базах дает возможность выделить наиболее значимые атрибуты, что позволит в дальнейшем решить задачу интеграции (объединения) этих баз для повышения эффективности их применения в системах анализа защищенности компьютерных систем и сетей.*

Ключевые слова *— защита информации, уязвимости, базы уязвимостей, тенденции обнаружения уязвимостей, анализ защищенности, компьютерные атаки, программно-аппаратное обеспечение.*

Введение

За последние десятилетия зависимость современного общества от компьютерных систем существенно возросла. Банковские операции, управление торговлей рынков, автоматизированные военные и государственные системы все в большей степени зависят от компьютерных систем. В результате риск реализации различных классов атак, базирующихся на эксплуатации имеющихся уязвимостей в программно-аппаратном обеспечении, для критически важных объектов очень велик.

Как следствие, в наши дни проводятся крупномасштабные исследования проблем безопасности, вызванных уязвимостями программно-аппаратного обеспечения. Несмотря на существующие угрозы, общество не готово отказаться от использования сети Интернет и компьютерных сетей в целом, так как они предоставляют огромные возможности в финансовой, политической и военной сферах. Постоянное совершенствование технологий безопасности в информационном мире не может дать гарантий абсолютной защищенности компьютерных систем.

Уязвимости обнаруживались во всех основных операционных системах и приложениях. Так как новые уязвимости находят непрерывно, единственный путь уменьшить вероятность их использования злоумышленниками заключается в выполнении непрерывного мониторинга защищенности, заключающегося в постоянном отслеживании появления уязвимостей, оперативном установлении обновлений и использовании инструментов, которые помогают противодействовать возможным атакам, базирующимся на эксплуатации этих уязвимостей [1–6].

Классификации уязвимостей систематизируют различные виды искусственных и естественных, случайных и злонамеренных, внутренних и внешних угроз по множеству параметров. Как правило, имеющиеся системы классификации уязвимостей выделяют класс угроз, связанный с возможностью реализации нарушителем программных и аппаратных уязвимостей, однако классы уязвимостей описываются только в общем плане. При всем этом классификации уязвимостей являются основой для построения моделей угроз безопасности компьютерных сетей.

Уязвимости можно классифицировать по этапам жизненного цикла, на которых они появляются: 1) уязвимости этапа проектирования; 2) уязвимости этапа реализации; 3) уязвимости этапа эксплуатации. По объекту воздействия выделяются следующие типы уязвимостей: уровня сети; уровня операционной системы; уровня баз данных; уровня приложений [7]. Также можно классифицировать уязвимости по типу целевого средства, а именно: 1) аппаратных средств; 2) операционных систем; 3) приложений.

Первые инциденты нарушения безопасности, официально зарегистрированные в базах данных уязвимостей, появились в 1988 г. С тех пор ведется постоянный поиск и регистрация уязвимостей как в рамках различных открытых проектов, так и коммерческими компаниями, исследовательскими институтами и добровольцами. Среди лидеров детектирования уязвимостей можно выделить компанию MITRE и ее базу «Общие уязвимости и воздействия» (Common Vulnerabilities and Exposures — CVE) [8], Национальный институт стандартов и технологий (National Institute of Standardsand Technology — NIST) и его «Национальную базу данных уязвимостей» (National Vulnerabilities Database — NVD) [9], проект «Открытая база данных уязвимостей» (Open Source Vulnerabilities Data Base — OSVDB) [10], Группу чрезвычайного компьютерного реагирования Соединенных Штатов (United State Computer Emergency Readiness Team — US-CERT) с «Базой данных записей уязвимостей» (Vulnerability Notes Database — VND) [11], проект SecurityFocus и его ленту уязвимостей BugTraq [12], компанию IBM с базой уязвимостей X-Force [13], а также коммерческие («закрытые») базы компаний Secunia [14] и VUPEN Security [15].

Представляемые в статье результаты анализа открытых баз уязвимостей были получены в рамках разработки интегрированной базы уязвимостей. Практическая реализация данной базы в дальнейшем будет использоваться в качестве компонента системы оценки защищенности компьютерных сетей [4]. Все полученные статистические данные были собраны посредством автоматизированной обработки информации каждой используемой базы, ее дальнейшего разбора и анализа.

Проведенное исследование позволяет получить ясную картину в области обнаружения уязвимостей, что, в свою очередь, дает возможность проводить оценки качества производимых продуктов различных мировых компаний, а также сравнивать по степени безопасности как типы программно-аппаратного обеспечения, так и конкретные решения, вышедшие на рынок.

Открытые базы уязвимостей

Для получения представления о содержании открытых баз данных уязвимостей необходимо произвести их анализ. В качестве основных были выбраны следующие источники: CVE, NVD, OSVDB, база уязвимостей X-Force.

База уязвимостей CVE и переход к формату CVRF

База данных уязвимостей CVE ведется с 1999 г. и на 5 мая 2014 года включала 70 078 записей. Основное отличие данной базы заключается в том, что она является наиболее полной и систематизированной, поэтому ее используют как основу для указания соответствия записей уязвимостей в других базах.

К основным полям (элементам структуры) записей уязвимостей относятся:

1) статус — в этом поле может содержаться либо значение Entry (проверенная запись), либо значение Candidate (еще не проверенная уязвимость);

2) фаза — в этом поле содержится значение этапа развития уязвимости, а также дата присвоения указанного этапа. В качестве значений могут быть: Proposed — фаза предложения уязвимости; Interim — промежуточная фаза уязвимости; Modified — фаза модификации уязвимости; Assigned — фаза установления уязвимости;

3) описание — поле содержит текстовое описание уязвимости;

4) ссылки — в данном поле содержатся ссылки на другие источники с указанием конкретного адреса интернет-ресурса описания уязвимости и идентификатора источника;

5) голоса — поле содержит имена членов голосования, принявших решение о занесении уязвимости в базу;

6) комментарии — в поле имеется имя автора комментария и его текстовое содержание.

Также в атрибутах записей уязвимостей содержится тип уязвимости, имя и идентификатор. Имя уязвимости имеет формат «*CVE-YYYY-NNNN*», где *YYYY* — это год обнаружения уязвимости, а *NNNN* — ее порядковый номер. У идентификатора уязвимостей в записи присутствует только год и порядковый номер.

Процесс добавления уязвимости в базу содержит три этапа:

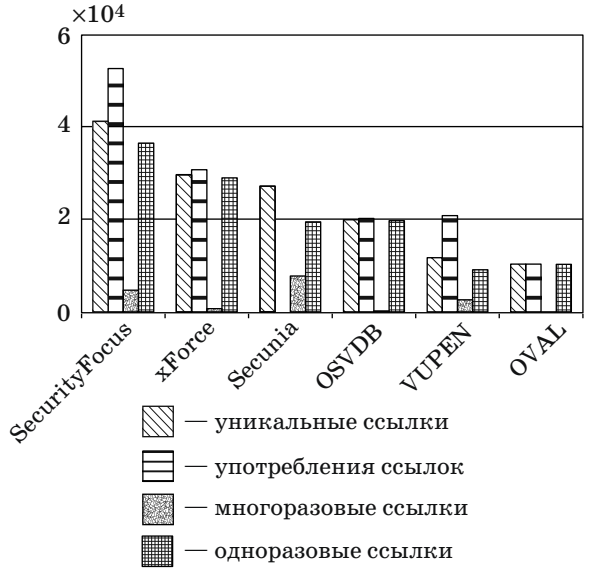
1) обработку — анализ, исследование и процесс приведения уязвимости к формату CVE;

2) присвоение — назначение конкретной записи уязвимости идентификатора CVE;

3) публикацию — добавление новой записи и публикация ее на интернет-ресурсе CVE [8], как только идентификатор CVE официально присвоен.

Статистика количества ссылок на сторонние источники в уязвимостях из базы CVE представлена на рис. 1. Стоит отметить, что наибольшее число ссылок ведет на ресурсы других баз данных уязвимостей, а остальные — на наиболее крупных производителей программно-аппаратного обеспечения.

Исходя из результатов анализа и полученной статистики связей с другими источниками, можно сделать вывод о том, что база данных уязвимостей CVE представляет собой достаточно полный список уязвимостей и имеет большое количество ссылок на базы уязвимостей и производителей программных и аппаратных средств. С другой



■ ***Рис. 1.*** Статистика использования ссылок на сторонние источники в базе CVE

стороны, в базе CVE отсутствует механизм описания принадлежности уязвимостей к конкретным продуктам, а также присвоение им метрик и расчета степени опасности.

В мае 2012 года был представлен формат «Общая структура сообщений об уязвимостях» (Common Vulnerability Reporting Framework — CVRF) [16], и сейчас происходит переход записей уязвимостей CVE на данный формат. Основными отличиями формата CVRF от формата CVE являются:

1) представление полей «Описание», «Этап добавления» и «Фаза» в едином элементе «Запись» (Note);

2) наличие у каждой записи уязвимости порядкового номера (атрибут Order), считая от начала составления базы CVE;

3) возможность привязки записей уязвимостей к списку продуктов, подвергающихся данной уязвимости.

Безусловно, все указанные изменения являются преимуществом формата CVRF, но вместе с тем наиболее явным достоинством обладает п. 3, описание которого будет приведено далее.

База уязвимостей NVD

Национальная база данных уязвимостей США (NVD) — хранилище данных уязвимостей, основанное на стандартах протокола автоматизации содержимого безопасности (Security Content Automation Protocol — SCAP). База NVD объединила в себе описание уязвимостей, названия программного обеспечения с этими уязвимостями и оценки опасности уязвимостей [17, 18]. На 5 мая 2014 года база данных уязвимостей NVD имела 62 124 записи уязвимостей.

Структура записи уязвимости в базе NVD является расширенной формой представления записи в базе CVE, за счет наличия следующих полей: 1) конфигурации уязвимых продуктов с учетом зависимостей; 2) списка уязвимых продуктов; 3) показателей, характеризующих уязвимость в формате «Общей системы оценки уязвимостей» (Common Vulnerability Scoring System — CVSS) версии 2.0 [19]; 4) типа доступа для реализации уязвимости.

В ходе исследования базы NVD было установлено, что 82,77 % уязвимостей принадлежат приложениям, и всего лишь 12,28 и 3,59 % — операционным системам и аппаратному обеспечению соответственно (рис. 2).

Также было выявлено, что зависимости конфигураций уязвимых продуктов (когда уязвимость характерна не для отдельного продукта, а для комбинации нескольких, например, операционной системы и приложения) встречаются лишь в 7,95 % всех записей уязвимостей (рис. 3).

■ ***Рис. 2.*** Статистика принадлежности записей по типу уязвимых продуктов

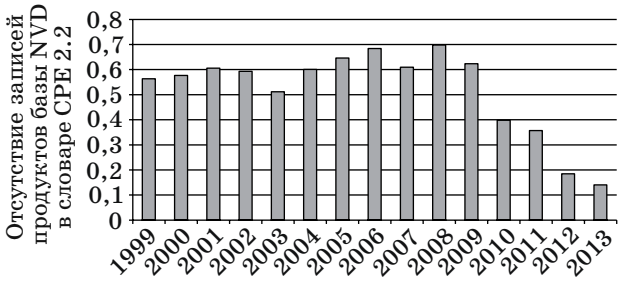
■ ***Рис. 3.*** Статистика распределения записей уязвимостей по наличию зависимостей продуктов, %

Основную часть зависимостей в конфигурациях составляют записи пар продуктов (например, приложения и операционной системы), а уязвимости, в которых больше чем один продукт влияет на ее успешную реализацию, встречаются около 30 раз, и, как правило, это некорректные записи.

Отличительной особенностью базы NVD от всех рассматриваемых баз уязвимостей является использование «Общего перечисления платформ» (Common Platform Enumeration — CPE) [20], являющегося одним из лучших словарей продуктов среди известных аналогов за счет большого числа записей и унифицированного формата имен программно-аппаратного обеспечения. Однако даже у данного формата представления записей продуктов есть недостатки, а именно: 1) неоднозначность значений разных полей формата; 2) недостаточное использование записей данного словаря базой NVD (рис. 4).

Первый недостаток был выявлен при выделении значений каждого из полей формата записи продуктов и дальнейшем сравнении со значениями смежных полей. Результаты анализа показали, что достаточно большое количество (около 70) значений разных полей пересекаются (равны), что приводит к неточному распознаванию неформатированных имен, а значит, точность определения наличия уязвимости по таким именам существенно падает. Второй недостаток заключается в неполноте (по количеству записей) словаря CPE, что было обнаружено в результате поиска в нем используемых в базе NVD записей продуктов.

Как было сказано ранее, формат CVRF имеет собственную структуру представления как словаря продуктов, так и механизма описания конфигураций уязвимого программно-аппаратного обеспечения. Главной особенностью данной структуры является ее иерархичность, которая обеспечивает более удобный доступ к данным, их представление и использование, чем в словаре CPE. Основа структуры (главный элемент) представлена полем «Ветка» (Branch), которое отвечает за соблюдение правил построения дерева



■ ***Рис. 4.*** Распределение отсутствующих записей продуктов из базы NVD в словаре CPE

продуктов. Таким образом, исключается дублирование данных, но, что более важно, это позволяет указывать в конфигурации уязвимых продуктов не только отдельные записи продуктов, но и группы продуктов, также имеющих свои идентификаторы. К сожалению, доступ к данному словарю в настоящий момент закрыт, в связи с чем провести качественный анализ и сравнение данного словаря со словарем CPE не удалось.

База уязвимостей OSVDB

Независимая и открытая база данных уязвимостей OSVDB создана для сообщества специалистов в области безопасности. Цель проекта состоит в том, чтобы обеспечить точную, детализированную, актуальную информацию об уязвимостях для систем обеспечения безопасности [21]. На 5 мая 2014 года данная база содержала 105 413 уязвимостей.

Структура данной базы не сильно отличается от ранее рассмотренной базы NVD, однако стоит отметить основные поля ее записи уязвимости: «Идентификатор OSVDB»; «Дата обнаружения»; «Имя производителя»; «Имя продукта»; «Версия продукта», которая содержит строковое значение версии продукта, имеющего данную уязвимость; «Ссылка», указывающая на прямой адрес к интернет-ресурсу другой базы или базы производителя, в котором описывается данная уязвимость; «Решение», имеющее строковое описание «исправления» уязвимости; «Метрики уязвимости», содержащие критерии оценки уязвимостей в формате CVSS версии 2.0; это поле не является обязательным (ввиду того, что поле присутствует при наличии ссылки на базу NVD).

База уязвимостей X-Force

База уязвимостей X-Force является проектом компании IBM и находится в открытом доступе в сети Интернет. Поля данных, описывающих записи уязвимостей этой базы, не сильно отличаются от полей баз уязвимостей, описанных ранее. Однако в их состав входят элементы, указывающие на преимущество базы X-Force: поле «Последствия», выражающее в формализованном виде возможный результат эксплуатации уязвимости; поле TemporalScore, являющееся элементом системы метрик CVSS, используемой для оценивания временных характеристик уязвимости. Также стоит отметить наличие в базе довольно подробных описаний и заключений об уязвимостях.

На 19 мая 2014 года база содержала 65 550 записей уязвимостей, 69,19 % из которых имеют базовую и временную оценки системы показателей CVSS, характеризующих данные уязвимости. Описания уязвимостей также содержат параметр, определяющий риск, которому подвергается система при реализации конкретной

уязвимости. Уязвимости низкого уровня опасности составляют всего 12 %, а на уязвимости среднего и высокого уровня опасности приходится 82 % (62 и 26 % соответственно), что определяет существующую проблему как в области разработки программно-аппаратного обеспечения, так и в области его безопасного использования.

В результате анализа уязвимостей по базовой и временной оценкам системы CVSS было получено распределение записей по шкале от 1 до 10 (рис. 5).

На рисунке x — это текущий диапазон значений для базовых и временных оценок. Стоит отметить, что наибольшее число уязвимостей имеет по базовым показателям оценку от 4 до 8, а по временным показателям — от 3 до 8, с максимами в диапазонах значений от 3 до 4 и от 4 до 5 соответственно.

При сравнительном анализе рассматриваемых баз данных уязвимостей по количеству ссылок на источники описания уязвимостей было установлено, что лидером является база OSVDB с результатом в среднем 11,5 ссылок на уязвимость, далее следует база X-Force — 6 ссылок на уязвимость и, наконец, базы CVE/NVD/CVRF со значением в среднем 5,6 ссылок на уязвимость.

■ ***Рис. 5.*** Распределение уязвимостей базы X-Force по базовой и временной оценкам системы CVSS

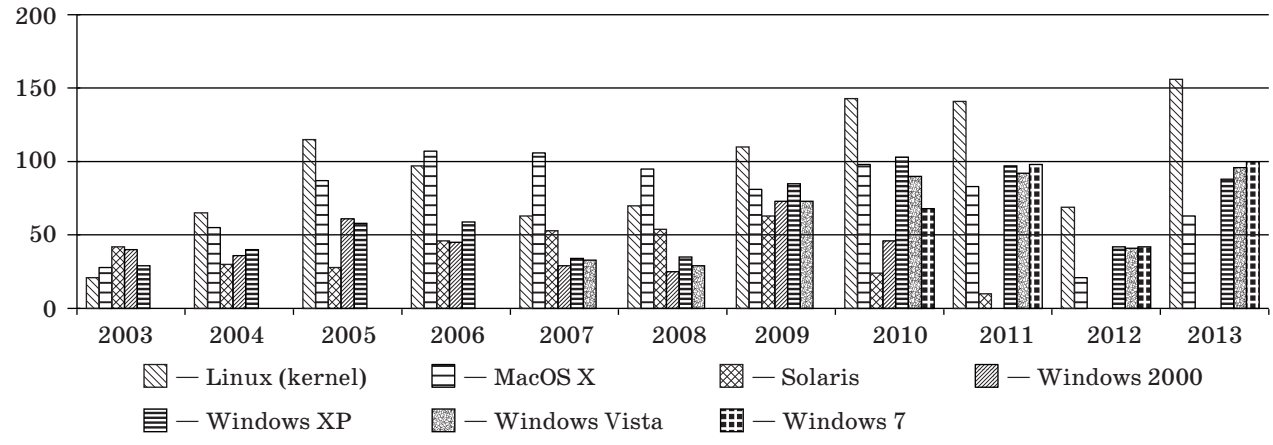
Тенденции в области обнаружения уязвимостей программно-аппаратного обеспечения

По общему числу зарегистрированных в базе NVD уязвимостей за последние 10 лет можно выделить следующих производителей программно-аппаратного обеспечения: 1) Microsoft (4,67 %); 2) Apple (3,93 %); 3) Oracle (3,65 %); 4) IBM (3,08 %); 5) Cisco (2,65 %); 6) Sun (2,33 %); 7) Mozilla (2,28 %); 8) Linux (1,99 %); 9) Google (1,88 %); 10) HP (1,59 %); 11) RedHat (1,11 %); 12) Apache (0,77 %).

В ходе сравнения числа уязвимостей операционных систем было выявлено, что на один продукт семейства Windows в среднем в год приходится 60 уязвимостей, Mac OS X — 75, Linux (kernel) — 95.

Распределение уязвимостей в клиентских операционных системах представлено на рис. 6. По данному рисунку видно, что в последние 5 лет наиболее уязвимым является ядро операционных систем Linux, более безопасными по количеству уязвимостей являются операционные системы корпорации Microsoft и наименьшее число уязвимостей в данный момент обнаруживается в операционной системе Mac OS компании Apple.

В ходе исследования открытых баз уязвимостей был проведен анализ уязвимостей по их принадлежности к конкретным типам продуктов: 1) операционные системы (клиентские); 2) серверные операционные системы и 3) веб-браузеры. Из полученных результатов можно выделить то, что на протяжении всего времени большее количество уязвимостей детектируется



■ ***Рис. 6.*** Распределение уязвимостей среди операционных систем

в программном обеспечении первого типа (исключением является 2011 г., в который по числу уязвимостей лидирует третий тип продуктов). Также за рассматриваемый временной интервал количество уязвимостей во всех трех типах продуктов сохраняется на довольно высоком уровне (рис. 7).

Стоит отметить, что в 2012 г. Microsoft значительно уступила по числу обнаруженных уязвимостей таким компаниям, как Mozilla, Cisco, IBM, Apple и Oracle, хотя до 2011 г. данная компания являлась абсолютным лидером по числу уязвимостей (рис. 8).

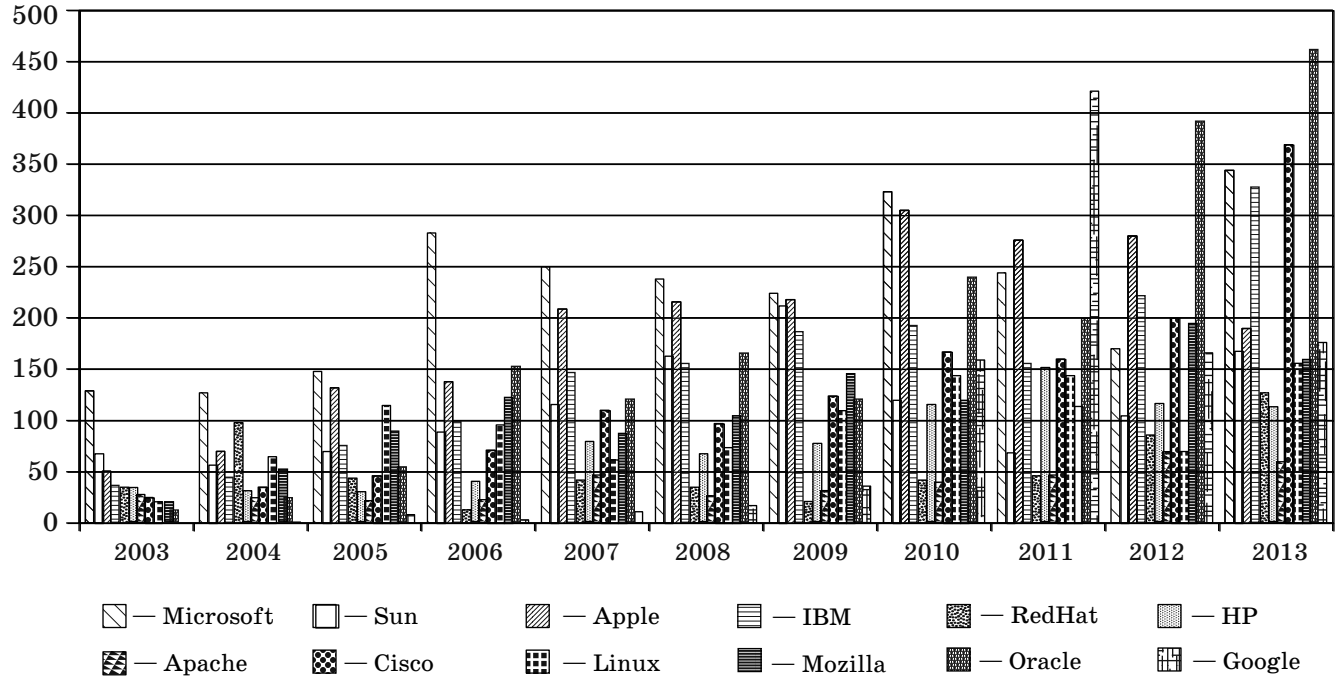
■ ***Рис. 7.*** Распределение уязвимостей однотипных продуктов

Это обусловлено тем, что в последние годы происходит активное перераспределение рынка программно-аппаратного обеспечения. В свою очередь, стремительный рост количества уязвимостей в продуктах компании Oracle можно объяснить покупкой Java в 2010 г. Резкий скачок в 2011 г. числа уязвимостей в продуктах компании Google объясняется выпуском браузера Chrome, который являлся самым уязвимым продуктом в 2010 и 2011 годах.

Проведенное исследование открытых баз уязвимостей дало ясную картину развития и текущего состояния в области уязвимостей программно-аппаратного обеспечения. Опираясь на полученные результаты, можно сделать вывод, что в данный момент происходят положительные изменения (более точное детектирование уязвимостей; работы над новыми форматами записей уязвимостей и продуктов; увеличение количества уязвимостей, подвергшихся оцениванию по различным показателям).

Вместе с тем отрицательно сказывается сохранение существующих недостатков баз уязвимостей — отсутствие форматов записей продуктов (базы OSVDB и X-Force), невозможность прямой загрузки баз уязвимостей. Исходя из данных фактов нельзя судить однозначно ни об общем улучшении баз уязвимостей, ни о качестве их использования в различных системах безопасности.

В свою очередь именно множественные несоответствия форматов описания уязвимостей и продуктов, а также несогласованное составление баз уязвимостей привело авторов настоящей ста-



■ ***Рис. 8.*** Распределение уязвимостей крупнейших производителей программно-аппаратного обеспечения

тьи к необходимости создания интегрированной базы уязвимостей, которая должна собрать в себе только полезную информацию, необходимую для более эффективного функционирования разрабатываемой системы оценки защищенности компьютерных сетей [4].

Заключение

В результате проделанного анализа можно сделать вывод о том, что, несмотря на большое количество баз данных уязвимостей, каждая база имеет выраженные преимущества и недостатки. В свою очередь накопление информации об уязвимостях и их возрастающее количество в настоящее время может привести к большим несогласованностям между имеющимися базами данных уязвимостей в будущем, что усложнит их использование отдельно друг от друга. Тенденции в области обнаружения уязвимостей в различных продуктах дают понять, что основная масса программно-аппаратного обеспечения, подвергающего систему высокому риску нарушения безопасности, принадлежит лидирующим компаниям. Вместе с этим их популярность среди пользователей только увеличивает шансы на успешную эксплуатацию той или иной уязвимости, что указывает на недостаточную защищенность данных продуктов и ставит под сомнение их репутацию в рамках обеспечения должного уровня безопасности.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт № 2.2), проекта ENGENSEC программы Европейского сообщества TEMPUS и государственных контрактов № 14.604.21.0033 и 14.604.21.0137.

Литература

1. **Kotenko I. V., Stepashkin M. V.** Network Security Evaluation Based on Simulation of Malefactor's Behavior // Proc. of the Intern. Conf. on Security and Cryptography, (SECRYPT 2006), Portugal, Aug. 7–10, 2006. P. 339–344.
2. **Котенко И. В., Степашкин М. В., Богданов В. С.** Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 7–24.
3. **Ruiz J. F.**, at al. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components/ J. F. Ruiz, R. Harjani, A. Mana, V. Desnitsky, I. V. Kotenko, A. A. Chechulin // Proc. of the 20th Euromicro Intern. Conf. on Parallel, Distributed and Network-Based Processing (PDP 2012), Garching, Germany, 2012. P. 261–268.
4. **Kotenko I. V., Chechulin A. A.** Common Framework for Attack Modeling and Security Evaluation in SIEM Systems // Proc. of IEEE Intern. Conf. on Green Computing and Communications, Conf. on Internet of Things, and Conf. on Cyber, Physical and Social Computing, Besanson, France, Sept. 11–14, 2012. Los Alamitos, California, USA: IEEE Computer Society, 2012. P. 94–101.
5. **Чечулин А. А., Котенко И. В.** Комбинирование механизмов защиты от сканирования в компьютерных сетях // Информационно-управляющие системы. 2010. № 6. С. 21–27.
6. **Котенко И. В., Новикова Е. С.** Визуальный анализ для оценки защищенности компьютерных сетей // Информационно-управляющие системы. 2013. № 3. С. 55–61.
7. **Компьютерная** безопасность: вопросы и решения. http://comp-bez.ru/?p=782 (дата обращения: 06.06.2014).
8. **Common** Vulnerabilities and Exposures (CVE). http://cve.mitre.org (дата обращения: 06.06.2014).
9. **National** Vulnerabilities Database (NVD). http://nvd.nist.gov (дата обращения: 06.06.2014).
10. **Open** Source Vulnerabilities Data Base (OSVDB). http://osvdb.org (дата обращения: 06.06.2014).
11. **United** States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov (дата обращения: 06.06.2014).
12. **BugTraq.** http://securityfocus.com (дата обращения: 06.06.2014).
13. **X-Force.** http://xforce.iss.net (дата обращения: 06.06.2014).
14. **Secunia.** http://secunia.com (дата обращения: 11.10.2013).
15. **Vupen** Security. http://www.vupen.com (дата обращения: 25.05.2014).
16. **Common** Vulnerability Reporting Framework (CVRF). http://www.icasi.org/cvrf-1.1 (дата обращения: 06.06.2014).
17. **Common** Vulnerability Scoring System. http://www.first.org/cvss (дата обращения: 06.06.2014).
18. **Котенко И. В., Дойникова Е. В.** Система оценки уязвимостей CVSS и ее использование для анализа защищенности компьютерных систем // Защита информации. Инсайд. 2011. № 5. С. 54–60.
19. **Котенко И. В., Дойникова Е. В.** Анализ протокола автоматизации управления данными безопасности SCAP// Защита информации. Инсайд. 2012. № 2. С. 56–63.
20. **Common** Platform Enumeration (CPE). http://cpe.mitre.org (дата обращения: 05.06.2014).
21. **Open** Source Vulnerabilities Data Base (OSVDB). http://osvdb.org/about (дата обращения: 05.06.2014).

UDC 004.056

Open Vulnerability Bases and their Application in Security Analysis Systems of Computer Networks

Fedorchenko A. V.[a], Junior Researcher, fedorchenko@comsec.spb.ru
Chechulin A. A.[a], PhD, Tech., Senior Researcher, chechulin@comsec.spb.ru
Kotenko I. V.[a], Dr. Sc., Tech., Head of Laboratory of Computer Security Problems, ivkote@comsec.spb.ru
[a]Saint-Petersburg Institute of Informatics and Automation of RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation

Purpose: The amount of disclosed vulnerabilities in popular software and hardware stays high from year to year. At the same time, the lack of coordination between companies and communities which detect and classify vulnerabilities reduces the efficiency of vulnerability databases applicability in security analysis systems. The goal of the study is analyzing the open vulnerability bases and the assessment of their possible application in computer network security analysis systems, including the acquisition of statistic data and elicitation of the main trends in vulnerability detection. **Results:** Several open vulnerability databases (namely, CVE, NVD, X-Force and OSVDB) were analized and compared, as well as software/hardware dictionaries (like CPE) and vulnerability metrics (like CVSS). Statistic data were collected on disclosed vulnerabilities in popular operation systems and web browsers, showing the distribution of vulnerable products of the major software makers for the last 10 year. For the most popular products (from Microsoft, Google, Oracle, Apple, etc.), the general tendencies in detecting, publishing and patching vulnerabilities were displayed and discussed. **Practical relevance:** The analysis of vulnerability representation formats in open databases enables us to pick out the most significant attributes. This can help develop an approach to the integration of these databases, increasing the efficiency of their usage in security analysis systems for computer systems and networks.

Keywords — Information Security, Vulnerabilities, Vulnerability Databases, Tendencies of Vulnerabilities Detection, Security Analysis, Computer Attacks, Hardware and Software.

References

1. Kotenko I. V., Stepashkin M. V. Network Security Evaluation Based on Simulation of Malefactor's Behavior. *Proc. Int. Conf. "Security and Cryptography"*, Portugal, 2006, pp. 339–344.
2. Kotenko I. V., Stepashkin M. V., Bogdanov V. S. Architectures and Models of Active Vulnerabilities Analysis Based on Simulation of Malefactors' Actions. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2006, no. 2, pp. 7–24 (In Russian).
3. Ruiz J. F., Harjani R., Mana A., Desnitsky V., Kotenko I. V., Chechulin A. A. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components. *Proc. 20th Euromicro Int. Conf. "Parallel, Distributed and Network-Based Processing (PDP-2012)"*. Garching, Germany, 2012, pp. 261–268.
4. Kotenko I. V., Chechulin A. A. Common Framework for Attack Modeling and Security Evaluation in SIEM Systems. *Proc. IEEE Int. Conf. "Green Computing and Communications, Internet of Things, and Cyber, Physical and Social Computing"*. Besanson, France, 2012, pp. 94–101.
5. Chechulin A. A., Kotenko I. V. Combining Scanning Protection Mechanisms in Computer Networks. *Informatsionno-upravliaiushchie sistemy*, 2010, no. 6, pp. 21–27 (In Russian).
6. Kotenko I. V., Novikova E. S. Visual Analysis of Computer Network Security Assessment. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 3, pp. 55–61 (In Russian).
7. *Komp'iuternaia bezopasnost': voprosy i resheniia* [The Computer Security: Answers and Solutions]. Available at: http://comp-bez.ru/?p=782 (accessed 5 June 2014).
8. *Common Vulnerabilities and Exposures (CVE)*. Available at: http://cve.mitre.org (accessed 5 June 2014).
9. *National Vulnerabilities Database (NVD)*. Available at: http://nvd.nist.gov (accessed 5 June 2014).
10. *Open Source Vulnerabilities Data Base (OSVDB)*. Available at: http://osvdb.org (accessed 5 June 2014).
11. *United States Computer Emergency Readiness Team (US-CERT)*. Available at: http://www.us-cert.gov (accessed 5 June 2014).
12. *BugTraq*. Available at: http://securityfocus.com (accessed 5 June 2014).
13. *X-Force*. Available at: http://xforce.iss.net (accessed 5 June 2014).
14. *Secunia*. Available at: http://secunia.com (accessed 11 October 2013).
15. *Vupen Security*. Available at: http://www.vupen.com (accessed 25 May 2014).
16. *Common Vulnerability Reporting Framework (CVRF)*. Available at: http://www.icasi.org/cvrf-1.1 (accessed 5 June 2014).
17. *Common Vulnerability Scoring System*. Available at: http://www.first.org/cvss (accessed 5 June 2014).
18. Kotenko I. V., Doynikova E. V. Vulnerabilities Scoring System CVSS and its Application for the Computer Systems Security Analysis. *Zashchita informatsii. Insaid*, 2011, no. 5, pp. 54–60 (In Russian).
19. Kotenko I. V., Doynikova E. V. SCAP Protocol Overview. *Zashchita informatsii. Insaid*, 2012, no. 4, pp. 54–66 (In Russian).
20. *Common Platform Enumeration (CPE)*. Available at: http://cpe.mitre.org (accessed 5 June 2014).
21. *Open Source Vulnerabilities Data Base (OSVDB)*. Available at: http://osvdb.org/about (accessed 5 June 2014).