DOI 10.36622/1682-7813.2025.28.1.011
УДК 004.056

УСОВЕРШЕНСТВОВАННАЯ МЕТОДИКА АВТОМАТИЗИРОВАННОГО СБОРА ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БЕСПРОВОДНЫХ СЕТЕЙ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, П.А. Анцупов, А.Г. Чурсин, И.О. Толстых

Целью исследования является совершенствования методики автоматизированного сбора информации об уязвимостях программного обеспечения беспроводных сетей Интернета вещей. Актуальность работы обуславливается использованием большого количества различных беспроводных технологий, использующихся для построения сетей Интернета вещей и необходимостью защиты конфиденциальной информации посредством сбора информации об уязвимостях программного обеспечения беспроводных сетей. В работе предложен метод статистического анализа описаний, по ключевым словам, для формирования базы данных ключевых слов. Полученные результаты могут быть использованы при разработке специализированного программного обеспечения применимого для сбора, приведения к общей структуре хранения и дополнения информации для дальнейшей работы с ней.

Ключевые слова: атака, IoT, CVSS 3.1, автоматизированный сбор информации, статистический анализ, база данных, Интернет вещей.

Введение

В сетях Интернета вещей (IoT) в настоящее время используется большое разнообразие беспроводных технологий и различное программное обеспечение (ПО).

При эксплуатации ПО в беспроводных сетях IoT, при идентификации пользователя как легитимного участника информационного ресурса предоставляется конфиденциальная информация, включающая:

- адреса электронной почты;
- логины и пароли учетных записей.

В первом квартале 2024 года количество кибератак увеличилось на 7 % по сравнению с предыдущим кварталом. Одним из наиболее распространенных последствий успешных кибератак вновь стала утечка конфиденциальной информации [1].

Наличие многочисленных уязвимостей в системном и прикладном ПО сетей Интернета вещей, позволяет выявлять конфиденциальную информацию как путем несанкционированного доступа, так и путем перехвата информации при ее передаче по беспроводным сетям.

Использование беспроводных технологий в сетях IoT предполагает использование вспомогательного программного обеспечения для защиты конфиденциальной информации. Но поскольку при разработке защитного ПО применяются сторонние библиотеки, фреймворки, API и аппаратные платформы, то невозможно предсказать все возможные пути получения несанкционированного доступа к данным [2].

В интересах парирования рисков несанкционированного воздействия на информационные системы в том числе сети Интернета вещей, были созданы специализированные базы данных (БД), которые содержат в себе информацию об известных уязвимостях с рекомендациями по устранению в случае их обнаружения [3], основными БД являются NVD (National Vulnerability Database) и Vulners.

Аналогично были созданы базы знаний эксплойтов – специальных программ, используемых для реализации несанкционированных действий путем эксплуатации тех или иных уязвимостей, в том числе с предоставлением доступа к программам, фрагментам программного кода, к наборам исполняемых команд и т.д. Так как базы находятся в режиме открытого доступа, злоумышленники также могут получать

доступ к ним и поддерживать свои знания в актуальном виде [4-5].

В этих условиях разработчикам системного и прикладного ПО крайне важно не только использовать информацию об известных уязвимостях и эксплойтах, содержащуюся в базах данных, оценивать риски реализации угроз путем эксплуатации таких уязвимостей, но и отслеживать информацию о новых уязвимостях, сведения о которых в базах отсутствуют (так называемых уязвимостях «нулевого дня»).

Анализ существующих сканеров безопасности

Подробнее следует рассмотреть существующие сканеры безопасности, обеспечивающие своевременное детектирование и выполнение мер по устранению уязвимостей программного обеспечения беспроводных сетей Интернета вещей.

ScanOVAL – это сканер безопасности, который использует в своей работе обширную базу данных OVAL-описаний – конфигурационной информации об уязвимом программном обеспечении (уязвимые программные продукты и версии, архитектура операционной системы и другое). Эти описания могут быть получены из открытых репозиториев, где любой желающий может предложить свою интерпретацию OVAL-описания на основе набора данных, содержащихся в базах данных уязвимостей программного обеспечения и эксплойтов (NVD, Exploit-DB, MITRE, Vulners, Github и других) или собственных исследований, которое проверяется командой модераторов и другими членами сообщества.

IBM QRadar Vulnerability Manager – это программное средство, разработанное компанией IBM, которое позволяет в режиме реального времени проводить анализ, аналитику, сканирование и менеджмент по устранению уязвимостей. В ходе проведения анализа на наличие уязвимого программного обеспечения, используемого в распределенной компьютерной сети, IBM QRadar использует обширные наборы данных, полученные из NVD и собственной базы знаний IBM X-Force Threat Intelligence, и по результатам проведенного исследования предлагает меры по их устранению с указанием приоритета очередности их исправления.

Rapid7 Nexpose – это бесплатный сканер безопасности, разработанный компанией Rapid7, которая является крупнейшим поставщиком унифицированных решений для управления уязвимостями. Данный продукт предназначен для предприятий с крупномасштабными распределенными сетями. Основными целями данного прикладного программного обеспечения являются: определение приоритетов, эффективное управление рисками, а также обеспечение безопасности информационных систем.

X-Scan – это многопоточный сканер уязвимостей, который позволяет искать уязвимые аппаратные ресурсы к определенным эксплоитам в заданном диапазоне IP-адресов.

Помимо сканирования уязвимостей необходимо также выделять, обрабатывать и передавать разработчикам и аналитикам безопасности информацию об уязвимостях в корректном виде. Методы поиска, обработки и предоставления вендорам таких сведений быстро развиваются во всем мире, в том числе в рамках широко известной сегодня технологии Data Mining, разработанной американскими специалистами. Однако сведения, касающиеся методов сбора и анализа уязвимостей ПО, применяемых в рамках указанной технологии, практически не раскрываются. Вместе с тем процедуры оценки уязвимостей ПО регламентированы целым рядом стандартов, основным из которых признан американский стандарт CVSS, вторая и третья версии которого сегодня применяются во всем мире и приняты в виде аутентичного перевода в качестве национальных стандартов в России. Однако для использования положений этих стандартов необходимы соответствующие исходные данные, объемы которых по всем классам защищаемых информационных систем крайне велики, что обусловливает неэффективность «ручного поиска» и необходимость автоматизации поиска, быстрой обработки и предоставления разработчикам ПО необходимых данных, что

сегодня представляет собой весьма нетривиальную задачу.

Усовершенствования методики автоматизированного сбора данных

В большинстве случаев, в базах данных уязвимостей изначально описание содержит неполный набор данных, в котором отсутствуют:

– вектор базовой оценки;

– список версий уязвимого программного обеспечения;

– идентификатор ошибки.

Современные сканеры безопасности используют в своей работе интегральную оценку опасности уязвимости в программном обеспечении, но получить прогноз о возможных ущербах уязвимости не представляется возможным из-за отсутствия информации о метриках вектора CVSS.

Исходя из выше проведенного анализа, ставится цель усовершенствования методики автоматизированного сбора данных об уязвимостях ПО беспроводных сетей Интернета вещей с использованием методов восполнения недостающей информации.

Для достижения этой цели выдвинуты три задачи:

1. осуществить анализ описаний уязвимостей, которые имеют полный набор данных;

2. сформировать базу данных ключевых слов;

3. осуществить корреляцию данных для предотвращения формирования вектора CVSS 3.1 с ложным набором метрик.

Основной принцип усовершенствованной методики автоматизированного сбора информации об уязвимостях ПО беспроводных сетей Интернета вещей заключается в анализе известных описаний уязвимости и эксплойта, использующего ее для реализации атаки на ПО беспроводных сетей Интернета вещей, на наличие специальных лексем, находящихся в базе данных и используемых при определении значений метрик базового вектора оценки CVSS 3.1. Следует выделить то что проводится исследование более, чем одного источника информации, следовательно повышается точность данных, так как различные источники содержат информацию, касаемо возможных оценок ущерба при получении доступа и возможной манипуляции с данными, а другие о вероятности реализации при подготовке к атаке на ПО с использованием исследуемой уязвимости.

Анализ описания уязвимостей с полным набором данных

Для решения первой задачи необходимо провести сбор информации из открытых баз данных об уязвимостях программного обеспечения, таких как: базы данных NVD и Vulners. Так как используются различные структуры предоставления информации, требуется предложить метод, адаптирующийся к ним, который будет использован в специально разработанном программном обеспечении, реализующем его (рис. 1, 2).

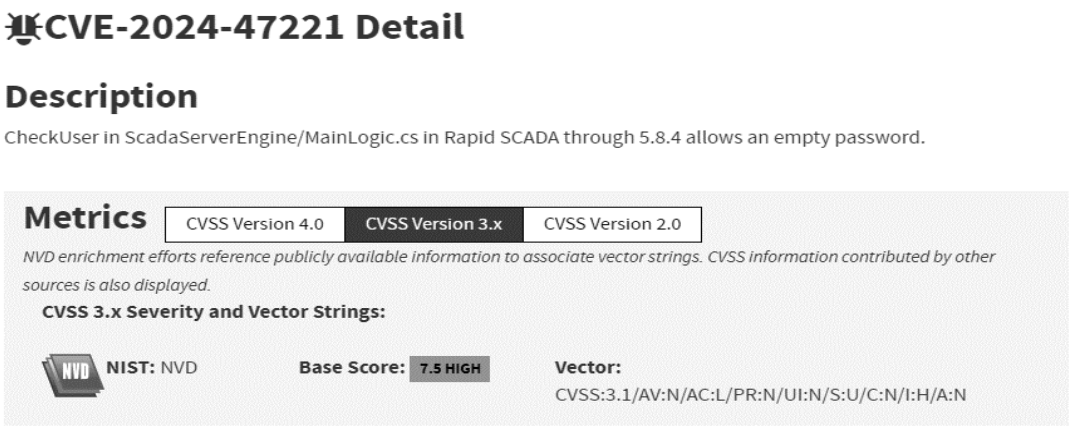

Рис. 1. Информация об уязвимости, взятая из базы данных NVD

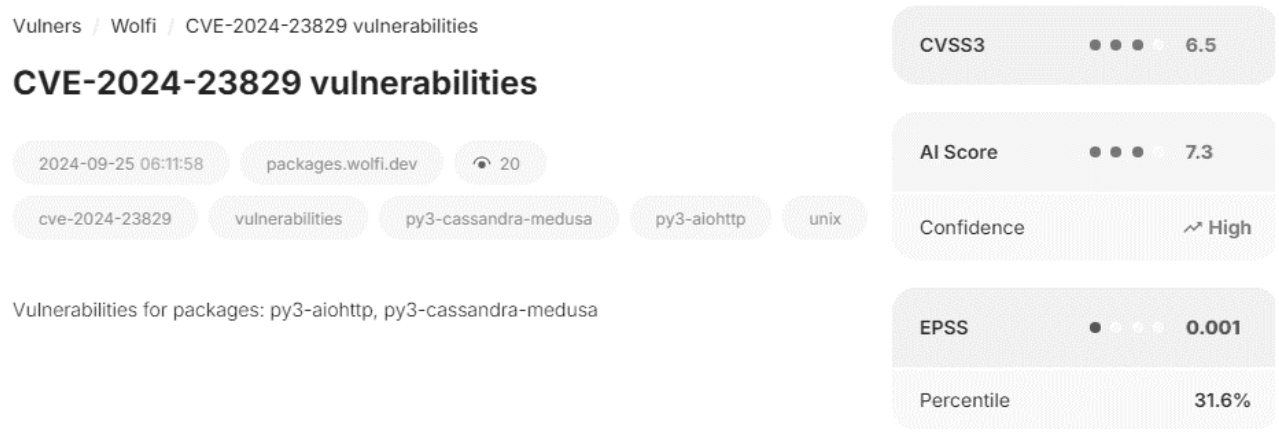

Рис. 2. Информация об уязвимости, взятая из базы данных Vulners

Для информационной структуры NVD характерны следующие данные:

- описание уязвимости;
- вектор уязвимости CVSS 2;
- вектор уязвимости CVSS 3.x;
- интегральные оценки критичности уязвимости.

Для информационной структуры Vulners характерны данные, используемые при описаниях NVD, а также:

- собственная оценка критичности уязвимости;
- информация об исследователе.

Формирование базы данных ключевых слов

Формирование базы данных ключевых слов для решения второй задачи – это процесс создания обширного репозитория терминов, используемых в описаниях уязвимостей программного обеспечения. Для этого необходимо провести тщательный статистический анализ описаний, чтобы выявить наиболее важные и часто встречающиеся ключевые слова, которые помогут в формировании полноценной базы данных., размещенных в базах данных NVD и Exploit-DB, при генерировании метрик базового вектора CVSS 3.1 (табл. 1, 2).

База данных Exploit-DB содержит следующую информацию:

- Уникальный идентификатор для поиска в хранилище, позволяющий быстро найти необходимые данные.
- Идентификатор для поиска в NVD, который играет ключевую роль в связывании информации из двух баз данных.
- Дата публикации, указывающая на момент, когда информация стала доступной для пользователей.
- Исходный код эксплойта, представляющий собой полноценный пример уязвимости программного обеспечения.
- Автор эксплойта, чье имя указывает на создателя данного эксплойта.
- Подтверждение EDB, подтверждающее аутентичность информации.
- Ссылка на файл с исходным кодом эксплоита, позволяющая пользователю скачать и изучить код.
- Уязвимая платформа, указывающая на тип программного обеспечения, которое может быть уязвимо.
- Ссылка для загрузки уязвимого программного обеспечения, позволяющая пользователю скачать и протестировать уязвимость.

Из перечисленных пунктов следует выделить следующие поля:

Идентификатор, используемый для поиска в NVD. Это поле необходимо для связи информации из двух баз данных, что обеспечивает полноту информации о уязвимостях программного обеспечения.

Уязвимая платформа. Этот параметр позволяет сузить диапазон поиска уязвимого программного обеспечения, что упрощает процесс поиска и анализа.

Исходный код эксплоита. В этом поле может содержаться информация о уязвимом программном обеспечении, включая название, версию, используемый язык программирования и алгоритм взаимодействия с конкретной уязвимостью.

Таблица 1

Примеры описаний, размещенных в базе данных NVD, используемых для формирования базы данных ключевых слов

Описание уязвимости	Базовый вектор CVSS 3.1								
	AV	AC	PR	UI	S	C	I	A	оценка
Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: MultiChannel Framework). Supported versions that are affected are 8.54 and 8.55. Easily "exploitable" vulnerability allows unauthenticated attac...	N	L	N	N	U	L	L	N	6.5
Vulnerability in the Oracle Customer Interaction History component of Oracle E-Business Suite (subcomponent: Admin Console). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily "exploitable" vulnerability allows unauthenticated att...	N	L	N	R	C	H	L	N	8.2

Таблица 2

Примеры описаний, размещенных в базе данных Exploit-DB, используемых для формирования базы данных ключевых слов

Описание эксплойта	Тип атаки
# Exploit Title: Duplicate Cleaner Pro 4 - Denial of Service (PoC) # Date: 2020-01-05 # Vendor Homepage:https://www.digitalvolcano.co.uk/index.html # Software Link: https://www.digitalvolcano.co.uk/download/DuplicateCleanerPro4_setup.exe # Exploit A...	dos
# Exploit Title: Small CRM 2.0 - Authentication Bypass # Google Dork: N/A # Date: 2020-01-02 # Exploit Author: FULLSHADE # Vendor Homepage: https://phpgurukul.com/ # Software Link: https://phpgurukul.com/small-crm-php/ # Version: V2.0 # Tested on:...	web
# Title: Linux/x86 - Execve() Alphanumeric Shellcode (66 bytes) # Date: 2019-12-31 # Shellcode Author: bolonobolo # Tested on: Linux x86 ########################## execve.asm ################################ global _start section .text _start:...	Shell code

Также проводится исключение незначимых описателей таких как предлоги, союзы, междометия и прочие слова, не несущие существенной смысловой нагрузки, с целью предотвращения создания ложных данных, при исследованиях критичности ущерба, используемого уязвимого программного обеспечения.

При проведении статистического анализа информации проводится разбиение исходных текстов описаний уязвимостей, характерных для каждого кода ошибки CWE (Common Weakness Enumeration), имеющего уникальное описание, на слова (табл. 3). Далее производится подсчет количества употреблений слов в исследуемых описаниях.

Таблица 3

Результат частотного анализа слов, употребляемых при описании уязвимостей с кодом ошибки CWE-287

Анализируемое слово	Количество применений
Login	8921
Password	7232
Port	5292
SQL	3092
WordPress	2345
QNAP	1985
…	
As	124
For	122

Корреляция данных для исключения ложных метрик

Далее следует провести корреляцию ключевых слов, полученных с применением статистического анализа, и описаний уязвимостей, характерных для каждого кода ошибки, с целью исключения лишних, использование которых может привести к генерации ложных сведений при формировании метрик, используемых в базовом векторе CVSS, стоит отметить, что показатели, которые наиболее важны при составлении описаний имеют большее число повторений, остальные данные необходимо исключить. На основе, полученных данных производится формирование базы данных ключевых слов, характерных для каждого кода ошибки CWE, данный этап обеспечивает решение третьей задачи.

Результаты

В результате проведенного исследования была предложена усовершенствованная методика автоматизированного сбора информации об уязвимостях программного обеспечения беспроводных сетей Интернета вещей. Данная методика формирует базу данных ключевых слов (табл. 4), используемых при описании уязвимостей, что является важных шагом в повышении точности и надежности анализа уязвимостей программного обеспечения IoT-систем.

Методика включает в себя несколько этапов. На первом этапе проводится анализ описаний уязвимостей с полным набором данных, доступных из открытых источников таких как базы данных уязвимостей.

На следующем этапе проводится формирование базы данных ключевых слов, характерных для каждой уязвимости. Для этого применяются методы текстового анализа. В итоге создается база данных, содержащая уникальные ключевые слова, связанные с каждой уязвимостью.

Третий этап методики включает проведении корреляции данных для предотвращения формирования вектора с ложным набором данных. При этом исключаются данные, имеющие наименьшее количество повторений. В результате этого этапа формируется более точный и надежный набор данных.

Таблица 4

Сформированная база данных ключевых слов, употребляемых при описании уязвимостей с кодом ошибки CWE-287

Анализируемое слово	Количество применений
Login	8921
Password	7232
Port	5292
SQL	3092
WordPress	2345
QNAP	1985

Практическое применение методики

Используя полученные результаты, можно осуществить проверку с целью получения достоверной информации на основании результатов проведенного исследования. Для апробации методики автоматизированного сбора информации об уязвимостях ПО сетей IoT будет использоваться уязвимость, имеющая идентификатор CVE-2019-20374 (рис. 3).

Описание, опубликованное в базе данных NVD, используется для проведения анализа с применением базы данных ключевых слов. По результатам исследования, была получена следующая информация:

- производится атака с внедрением вредоносного кода в редактор HTML-страницы (Вектор атаки - сетевой);
- уязвимость существует в определенных версиях программы Typora, которая распространяется на Linux и MacOS;
- результатом использования уязвимости осуществляется удаленное выполнение кода;
- эксплуатация проводится с помощью открытия специально сформированного файла, содержащего вредоносный код. Таким образом, требуется взаимодействие с пользователем уязвимой системы;
- осуществляется удаленное выполнение кода, следовательно, конфиденциальность, целостность и доступность информации может быть полностью нарушена
- удаленное выполнение кода может взаимодействовать с другими компонентами уязвимого программного обеспечения и повлиять на их работу;
- код ошибки уязвимости – CWE-79.

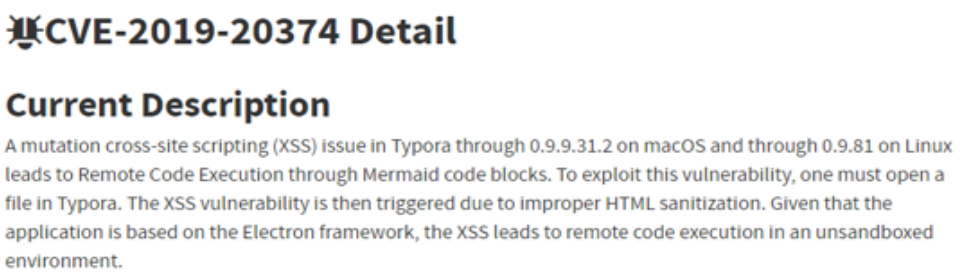

Рис. 3. Описание уязвимости CVE-2019-20374 в базе данных NVD

Также имеется ссылка на репозиторий GitHub, который содержит в себе программное решение, необходимое для исправления уязвимости и исходный код эксплойта. После проведенного анализа источника были получены следующие результаты:

- получены сведения об использовании файлов-сценариев с расширением .js, которые могут быть использованы в программном коде веб-страницы (Сложность атаки - низкая);

- даны рекомендации по использованию функции sanitize(), которая в качестве аргумента принимает вредоносный HTML-код и возвращает безопасный.

$$AV{:}N/AC{:}L/PR{:}N/UI{:}R/S{:}C/C{:}H/I{:}H/A{:}H \quad (1)$$

При помощи информации, собранной из выше исследованных источников, дано полное описание значений метрик, используемых в базовом векторе уязвимости по стандарту 3.1 (формула 1). При сравнении векторов, полученных с использованием разработанной методики и исследователями NVD (рис. 4), зафиксировано полное совпадение.

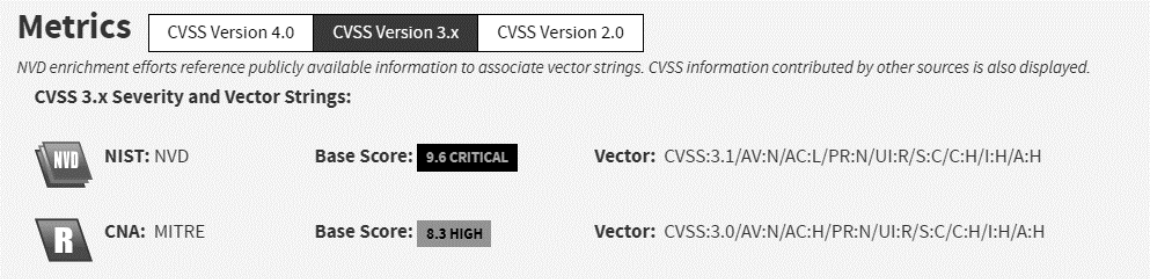

Рис. 4. Базовый вектор уязвимости CVE-2019-20374, опубликованный на сайте NVD

Заключение

В работе предложена усовершенствованная методика автоматизированного сбора информации об уязвимостях ПО сетей IoT, которая позволяет восполнять пробелы информации в уже имеющихся наборах данных и более точно формировать метрики базовых векторов уязвимости при их отсутствии.

Практическое применение предложенной методики заключается в возможности использования результатов при разработке специализированного программного обеспечения, задачей которого является сбор уже известных наборов данных, приведение к общей структуре хранения в базе данных, а также дополнения информации для дальнейшей работы с набором данных.

Методика имеет потенциал внедрения в системы Промышленного Интернета вещей в роли вспомогательного ПО.

Дальнейшее направление исследования состоит в использовании базы данных об уязвимостях программного обеспечения для разработки нейросетевых систем обнаружения атак на беспроводные сети.

Список литературы

1. Актуальные кибер угрозы: I квартал 2024 года. – Электрон. данные – Режим доступа: https://www.ptsecurity.com/ru ru/research/analytics/cybersecurity-threatscape-2024-q1/

2. Уязвимости и угрозы мобильных приложений в 2019 году. – Электрон. данные – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ mobile-application-security-threats-and-vulnerabilities-2019/

3. Vulners – гугл для хакера. Как устроен лучший поисковик по уязвимостям и как им пользоваться. – Электрон. данные – Режим доступа: https://xakep.ru/2016/07/08/vulners/

4. Exploit Database – Exploits for Penetration Testers, Researchers, and Ethical hackers – Электрон. дан. – Режим доступа: https://www.exploit-db.com

5. Ablon L., Bogart A. Zero days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits. – Rand Corporation, 2017.

Концерн «Созвездие», г. Воронеж
Concern «Sozvezdie», Voronezh

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 24.09.24

Информация об авторах

Ермаков Сергей Александрович – канд. техн. наук, начальник отдела, Концерн «Созвездие», г. Воронеж; доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Анцупов Павел Андреевич – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Чурсин Андрей Германович – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Толстых Ирина Олеговна – канд. техн. наук, старший инженер, Концерн «Созвездие», г. Воронеж; доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

AN IMPROVED TECHNIQUE FOR AUTOMATED COLLECTION OF INFORMATION ABOUT SOFTWARE VULNERABILITIES OF WIRELESS NETWORKS OF THE INTERNET OF THINGS

S.A. Ermakov, P.A. Antsupov, A.G. Chursin, I.O. Tolstykh

The purpose of the study is to improve the methodology of automated collection of information about software vulnerabilities of wireless networks of the Internet of Things. The relevance of the work is due to the use of a large number of different wireless technologies used to build Internet of Things networks and the need to protect confidential information by collecting information about software vulnerabilities of wireless networks. The paper proposes a method for static analysis of descriptions, by keywords, for the formation of a database of keywords. The results obtained can be used in the development of specialized software applicable for collecting, bringing to a common structure of storage and supplementing information for further work with it.

Keywords: attack, IoT, CVSS 3.1, automated information collection, statistical analysis, database, Internet of Things.

Information about the authors

Sergey A. Ermakov – Cand. Sc (Technical), Head of Department, Concern “Sozvezdie”, Voronezh; Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Pavel A. Antsupov – Graduate Student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Andrey G. Chursin – Graduate Student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Irina O. Tolstykh – Cand. Sc (Technical), Senior Engineer, Concern “Sozvezdie”, Voronezh, Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com