DOI 10.36622/VSTU.2023.26.3.021
УДК 004.45

КЛАССИФИКАЦИЯ УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С ПОВЫШЕНИЕМ ПРИВИЛЕГИЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ НА БАЗЕ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА LINUX, И ОЦЕНКА РИСКОВ ИХ ЭКСПЛУАТАЦИИ

А.Л. Сердечный, И.А. Каданцев, Д.И. Лоскутов

В работе проведена оценка и регулирование рисков для автоматизированных систем, связанных с возможностью повышения привилегий в операционных системах семейства Linux. Проведена классификация уязвимостей, связанных с повышением привилегий в автоматизированных системах на базе операционных систем семейства Linux, с учётом возможности количественного оценивания рисков, возникающих в результате эксплуатации таких уязвимостей. Предложена методика оценки рисков рассматриваемых рисков. Данная методика разработана на основе преобразования качественных метрик стандарта CVSS в количественные метрики, направленные на определение вероятности эксплуатации уязвимости и степени ущерба автоматизированной системе на базе операционной системы семейства Linux.

Ключевые слова: операционная система Linux, повышение привилегий, риск, уязвимость, повышение защищенности автоматизированной системы.

Введение

В современном обществе при обработке большого количества гигабайтов информации, ускорении производственных процессов, замене человеческого труда работой всевозможных автоматов применяются различного рода автоматизированные системы.

При автоматизации системы важным элементом этого процесса является ее программное обеспечение (далее – ПО). К ПО автоматизированной системы (далее – АС) в первую очередь стоит отнести операционную систему (далее – ОС).

Автоматизированные системы управления технологическими процессами (АСУ ТП) – это комплекс программных и технических средств, предназначенных для создания систем автоматизации управления технологическим оборудованием и производственными процессами на предприятиях. АСУ ТП – комплексное решение, обеспечивающее автоматизацию основных технологических операций на производстве в целом или каком-то его участке, выпускающем относительно завершенный. АСУ ТП может состоять из отдельных систем автоматического управления и комплексных устройств, объединенных единым решением для автоматизации технологических процессов с целью обеспечения максимальной эффективности решения производственных задач.

Для многих АС и АСУ ТП ставятся специфические задачи, решение которых возможно только при наличии специализированного ПО. Для этих целей часто применяют ОС Linux, которая, ввиду наличия открытого кода, может быть настроена под конкретные цели и задачи.

Linux (или GNU/Linux) – семейство Unix-подобных ОС на базе ядра Linux, включающих тот или иной набор утилит и программ проекта GNU. Linux-системы распространяются в виде различных дистрибутивов, имеющих свой набор системных и прикладных компонентов (как свободных, так и проприетарных) [1].

Поскольку ПО на базе Linux используется в значительном количестве различных областей, со стороны киберпреступников имеется прямая заинтересованность в поиске уязвимостей программного кода и написании программ для их эксплуатации, а разработчикам для минимизации влияния уязвимостей и ущерба от них необходимо обеспечивать

безопасность ПО как на прикладном уровне, так и на уровне ядра.

В настоящее время насчитывается значительное число механизмов и средств защиты, однако даже с учетом этого новые уязвимости ПО обнаруживаются и по сей день. Некоторые из них имеют высокую степень опасности. Уязвимости, используемые злоумышленником для того, чтобы повысить свои привилегии, могут находиться непосредственно в ядре ОС, поэтому эксплуатация таких уязвимостей может повлечь за собой большой ущерб пользователю системы.

Одной из самых распространенных целей эксплуатации уязвимостей программного обеспечения является повышение привилегий пользователя или программы, то есть получить доступ к ресурсам системы, которые недоступны с текущим уровнем привилегий. В результате нарушитель информационной безопасности АС может выполнять несанкционированные действия в рамках ОС.

Уязвимости, связанные с повышением привилегий в ОС Linux, в большей степени имеют высокий и критический уровень опасности, поскольку повышение привилегий чаще всего происходит за счет обхода механизмов защиты, встроенных в ядро ОС, а также по причине того, что повышение привилегий приводит к нарушению конфиденциальности, целостности и доступности информации.

При использовании ОС семейства Linux, в том числе их российских аналогов, актуальным является структурирование и актуализация данных об уязвимых компонентах ядра Linux для последующей оценки вероятности возникновения ущерба при эксплуатации существующих и потенциально возможных уязвимостей с высоким уровнем опасности, одними из которых являются уязвимости, связанные с повышением привилегий. Существующие данные об уязвимостях не содержат достаточного количества числовых данных, необходимых для расчета риска эксплуатации уязвимостей, поэтому для получения необходимых значений нужно преобразовать имеющиеся данные из качественных в количественные. Уязвимости, связанные с повышением привилегий в Linux, чаще всего направлены на один конкретный элемент структуры ядра ОС, а значит наличие средства защиты либо полностью исключает возможность эксплуатации уязвимости, либо уязвимость будет всегда работать в обход него [2].

Актуальность данного исследования обусловлена противоречиями, между:

- большим количеством сведений об уязвимостях, связанных с повышением привилегий и отсутствием структур данных об этих уязвимостях, позволяющих произвести комплексную оценку рисков эксплуатации уязвимостей на основе их связей и распространенности.
- необходимостью комплексной оценки рисков эксплуатации уязвимостей, приводящих к повышению привилегий в автоматизированных системах на базе ОС семейства Linux, и отсутствием адаптации методов оценки рисков к применению сведений о связях и распространению уязвимостей, связанных с повышением привилегий в ОС Linux.

Объектом исследования являются автоматизированные системы управления технологическими процессами на базе операционных систем семейства Linux, которые могут быть подвержены атакам, направленным на эксплуатацию уязвимостей, связанных с повышением привилегий.

Предметом исследования являются риски, связанные с эксплуатацией в автоматизированных системах уязвимостей, приводящих к повышению привилегий в операционных системах семейства Linux.

Целью исследования является повышение защищенности автоматизированных систем управления технологическими процессами на базе операционных систем семейства Linux за счет оценки и регулирования рисков эксплуатации уязвимостей, приводящих к повышению привилегий.

Для достижения поставленной цели на данном этапе исследования необходимо решить задачи:

- определить способы классификации сведений об уязвимостях, направленных на повышение привилегий в ОС семейства Linux, с учётом возможности

количественного оценивания рисков, возникающих в результате эксплуатации таких уязвимостей, с использованием сведений о связях и распространенности.

- определить способ оценки рисков эксплуатации уязвимостей, направленных на повышение привилегий в ОС семейства Linux, с использованием данных о связях и распространенности данных уязвимостей.

Классификация сведений об уязвимостях, направленных на повышение привилегий в операционных системах семейства Linux, с учётом возможности количественного оценивания рисков, возникающих в результате эксплуатации таких уязвимостей

В качестве выборки для классификации используются актуальные уязвимости, связанные с повышением привилегий в операционных системах семейства Linux, обнаруженные за три с половиной календарных года. Данные для определения необходимой для исследований выборки можно получить из различных баз данных уязвимостей, в частности из банка данных угроз безопасности информации ФСТЭК России [3] и из базы данных NVD [4]. Исходя из данных этой выборки можно заметить, что эксплуатация уязвимостей, связанных с этим, имеет высокое влияние на конфиденциальность, целостность и доступность информации в операционной системе и что многие уязвимости реализуются через компиляцию заранее подготовленного кода, который находятся в открытом доступе или распространяется в определенном круге людей.

Сочетание описанных факторов, а также иных факторов, описывающих конкретную уязвимость, дает общее представление об уровне опасностей уязвимостей, связанных с повышением привилегий в ОС семейства Linux. Оценка уязвимости стандартом CVSS показывает, насколько опасна данная уязвимость и насколько приоритетна задача ее исправления.

Помимо факторов, влияющих на оценку уровня опасности по CVSS, уязвимость характеризуется определением модулей ядра, которые являются уязвимыми, языка программирования, на котором написан уязвимый участок кода или же структуры уязвимой части системы. Помимо этого, практически каждая уязвимость характеризуется своим классом (или несколькими классами) ошибки, которая используется злоумышленником для эксплуатации. Самые распространенные типы ошибок среди рассматриваемых уязвимостей представлены в табл. 1.

Таблица 1

Самые распространенные типы ошибок, приводящих к повышению привилегий в операционных системах семейства Linux

Тип ошибки	Всего уязвимостей
CWE-416	68
CWE-787	38
CWE-269	24
CWE-362	23
CWE-476	16
CWE-190	13
CWE-20	10

Исходя из данных выборки, самыми распространенными являются типы ошибки CWE-416, CWE-787, CWE-269, CWE-362, CWE-476, CWE-190 и CWE-20.

Распределение уязвимостей по классам ошибок позволяет более наглядно увидеть, какие недостатки ПО приводят к возникновению уязвимости, а также понять, эксплуатация каких механизмов системы или программ позволяет повысить привилегии в Linux.

Проанализировав данную информацию, а также описание каждой уязвимости, можно получить четыре наиболее крупных класса уязвимостей, которые эксплуатируются с использованием схожих механизмов. Среди них действия за границами области памяти, некорректное освобождение памяти после использования, некорректный ввод данных и небезопасное управление привилегиями, а также можно выделить группу уязвимостей «другие», в которую включены уязвимости, которые невозможно определить в одну из групп и их число слишком мало.

Используя граф, отображающий связь уязвимостей с их типами ошибок, можно убедиться в достоверности данной

классификации. Инструментами средства визуализации и исследования графов Gephy с помощью алгоритма Лейдена получены кластеры, содержащие от одного до двух типов ошибок, связанных с определенным числом уязвимостей. В результате семь самых крупных типов ошибок расположены в рамках девяти самых крупных кластеров, включающих в себя также группу уязвимостей без выявленного конкретного типа ошибки и кластер, объединяющий типы ошибок CWE-119 и CWE-843. Полученная визуализация графа уязвимостей и их типов ошибок с выделенными наиболее крупными кластерами изображена на рис 1.

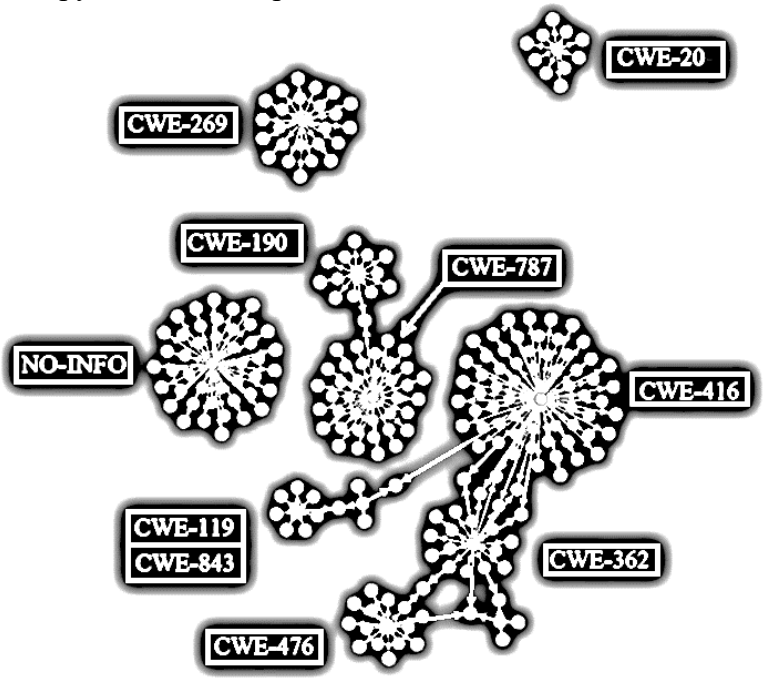

Рис. 1. Граф, содержащий распространенные типы ошибок уязвимостей, связанных с повышением привилегий в ОС Linux

Пример использования методики оценки рисков эксплуатации уязвимостей, связанных с возможностью повышения привилегий в операционных системах семейства Linux

В качестве методики оценки рисков эксплуатации уязвимостей, связанных с возможностью повышения привилегий в операционных системах семейства Linux используется методика, разработанная автором в рамках выпускной квалификационной работы.

Для каждой уязвимости существует базовый вектор оценки CVSS одной из версий. Он описывает направление и сложность атаки, а также степень влияния на систему и информацию. Среди метрик, используемых для оценки, можно выделить: вектор атаки, сложность атаки, необходимый уровень привилегий, необходимость взаимодействия с пользователем, влияние на другие компоненты системы, влияние на конфиденциальность, целостность или доступность информации.

Сочетание значений этих метрик, и подстановка в формулу для расчета базовой оценки CVSS позволяет определить уровень опасности конкретной уязвимости. Аналогично данные метрики можно использовать для оценки рисков эксплуатации уязвимостей. Вектор атаки, сложность атаки, уровень привилегий и необходимость взаимодействия с пользователем определяют вероятность эксплуатации уязвимости. Уровень влияния на конфиденциальность, целостность и доступность информации, а также на другие компоненты системы, определяет степень ущерба для организации в случае эксплуатации уязвимости. Соотношения качественных и количественных значений описанных метрик приведены в табл. 2 и 3.

Таблица 2

Численные значения метрик для определения вероятности эксплуатации уязвимости

Название метрики	Значения метрики			
Вектор атаки (AV)	Сетевой N (0,25)	Смежная сеть A (0,2)	Локальный L (0,15)	Физический P (0,05)
Сложность атаки (AC)	Высокая H (0,15)		Низкая L (0,25)	
Уровень привилегий (PR)	Высокий H (0,05)	Низкий L (0,2)	Не требуется N (0,25)	
Взаимодействие с пользователем (UI)	Требуется R (0,15)		Не требуется N (0,25)	

Таблица 3

Численные значения метрик для определения коэффициента величины ущерба при успешной эксплуатации уязвимости

Название метрики	Значения метрики		
Влияние на другие компоненты системы (S)	Не оказывает U (0)		Оказывает C (0,25)
Влияние на конфиденциальность (C)	Не оказывает N (0)	Низкое L (0,1)	Высокое H (0,25)
Влияние на целостность (I)	Не оказывает N (0)	Низкое L (0,1)	Высокое H (0,25)
Влияние на доступность (A)	Не оказывает N (0)	Низкое L (0,1)	Высокое H (0,25)

Для всех (не считая группы «другие») групп уязвимостей, связанных с повышением привилегий в АС на базе ОС семейства Linux, значения метрик влияния на конфиденциальность, целостность и доступность информации одинаковы. Значение данного вектора равно «AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H». Полученные сведения показывают, что в случаях, когда уязвимость можно отнести к одной из групп за исключением уязвимостей, эксплуатирующих «состояние гонки» и уязвимостей, которые нельзя отнести к какой-либо описанной группе, значения вероятностей эксплуатации уязвимостей, связанных с повышением привилегий в АС на базе ОС семейства Linux, и коэффициенты ущерба при успешной эксплуатации уязвимостей будут одинаковыми. Следовательно, для быстрой оценки риска возможности эксплуатации уязвимости можно использовать общие для все трех групп значения, когда уязвимость уже определена в одну из них, однако для более детальной оценки следует.

Для расчета абсолютной величины риска используется формула:

$$R_{(a)} = P(t) \cdot P(v) \cdot S, \qquad (1)$$

где P(t) – вероятность эксплуатации уязвимости;

P(v) – вероятность существования уязвимости;

S – уровень ущерба.

При этом значение S определяется по формуле:

$$S = k \cdot L, \qquad (2)$$

где k – коэффициент ущерба при успешной эксплуатации уязвимости,

L – максимальная величина возможного ущерба при успешной эксплуатации уязвимости злоумышленником.

Величины P(v) и L формул (1) и (2) определяются организацией или лицом, которые владеют АС. Величина P(v) равна отношению количества уязвимых АС к общему числу используемых АС. Величина L равна максимально возможному ущербу, который может понести организация или лицо, которые владеют АС, в случае успешной эксплуатации уязвимости злоумышленником [7].

Величина P(t) определяется как сумма значений метрик базового вектора, обозначающих вектор атаки, сложность атаки, необходимый уровень привилегий и необходимость взаимодействия с пользователем:

$$P(t) = k_{(AV)} + k_{(AC)} + k_{(PR)} + k_{(UI)},$$

где $k_{(AV)}$, $k_{(AC)}$, $k_{(PR)}$, $k_{(UI)}$ – соответствующие численные значения метрик базового вектора.

Величина k определяется как сумма значений метрик базового вектора, обозначающих влияние на конфиденциальность, целостность и доступность информации, а также на другие компоненты системы:

$$k = k_{(S)} + k_{(C)} + k_{(I)} + k_{(A)},$$

где $k_{(S)}$, $k_{(C)}$, $k_{(I)}$, $k_{(A)}$ – соответствующие численные значения метрик базового вектора.

Поскольку величины P(t), P(v) и k принимают максимальное значение равное единице, максимальное значение риска равно максимальному значению ущерба в случае успешной эксплуатации уязвимости злоумышленником:

$$R_{max} = L.$$

Относительная величина риска при этом вычисляется по формуле:

$$R = \frac{R_{(a)}}{R_{max}}.$$

Анализ уязвимости, связанной с повышением привилегий в операционных системах семейства Linux проведен относительно уязвимости BDU:2022-01567 (CVE-2022-27666) ядра операционной системы Linux, позволяющей нарушителю повысить права до уровня суперпользователя на уязвимом хосте.

В результате выполнения эксплойта пользователь получает привилегии на выполнение ранее недоступных команд, что свидетельствует об успехе применения эксплойта. Таким образом, уязвимость BDU:2022-01567 (CVE-2022-27666) может быть легко эксплуатирована на уязвимых версиях ОС Linux.

В соответствии с разработанной методикой проведены расчеты величины риска эксплуатации уязвимости, связанной с повышением привилегий в ОС семейства Linux. В качестве исходных значений базового вектора уязвимости BDU:2022-01567 (CVE-2022-27666) (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) используются $k_{(AV)}$=0,15, $k_{(AC)}$=0,25, $k_{(PR)}$ =0,2, $k_{(UI)}$=0,25, $k_{(S)}$=0, $k_{(C)}$=0,25, $k_{(I)}$=0,25, $k_{(A)}$=0,25. Помимо этого, значение вероятности существования уязвимости P(v)=0,5, так как считаем, что уязвимой является каждая вторая система. Значение максимальной величины возможного ущерба L=2000000.

В результате абсолютная величина риска эксплуатации уязвимости равно $R_{(a)}$=637500, а относительная величина риска R=0,31875. Полученное значение величины риска позволяет сделать вывод о том, что рассмотренная уязвимость может стать критичной для автоматизированной системы на базе уязвимой ОС Linux [8].

Развитие методики оценки рисков эксплуатации уязвимостей, связанных с возможностью повышения привилегий в операционных системах семейства Linux с использованием моделирования различных структур отображения данных

Поскольку уязвимости, содержащиеся в ОС, могут быть взаимосвязаны, например, по способам эксплуатации или же по уязвимым компонентам системы, оценивать риск эксплуатации одной конкретной уязвимости не всегда является целесообразным. Для этого необходимо создать структуры данных об этих уязвимостях, созданные с учетом конкретных признаков, которые можно отнести к каждой из уязвимостей, связанных с повышением привилегий в ОС семейства Linux. Примером таких признаков может служить разделение по механизмам защиты ядра ОС Linux. Фрагмент схемы, описывающий механизмы защиты ядра ОС Linux и их связь с типами уязвимостей и их классами ошибок представлен на рис. 2.

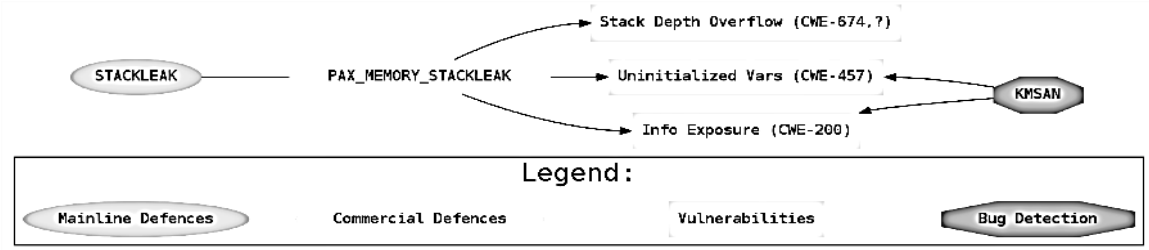

Рис. 2. Фрагмент схемы, описывающей связь механизмов защиты ядра ОС Linux с типами уязвимостей и их классами ошибок

Для наглядного отображения информации уместно в дальнейшем использовать метод информационной картографии. Если провести укладку графа с помощью необходимого алгоритма, можно не только визуально упростить восприятие большого объема данных, но и произвести расчеты необходимых для дальнейших исследований метрик, таких как коэффициент кластеризации и др.

Заключение

В работе рассмотрены риски, связанные с эксплуатацией в автоматизированных системах уязвимостей, приводящих к повышению привилегий в операционных системах семейства Linux.

Новизна полученных результатов заключается в следующем:

1. Впервые проведена классификация сведений об уязвимостях, связанных с повышением привилегий в автоматизированных системах на базе ОС семейства Linux, которая ориентирована на проведение риск-анализа возможности эксплуатации данных уязвимостей.

2. На основе полученной классификации сведений об уязвимостях, приводящих к повышению привилегий в автоматизированных системах на базе ОС семейства Linux, и методике оценки рисков информационной безопасности предложены способы применения методики в более обширных областях исследований.

Перечень сведений об уязвимостях, ориентированный на проведение риск-анализа, может быть повторно использован для аналогичных исследований в других типах систем. Полученная классификация сведений, ориентированная на проведение риск-анализа, может быть в дальнейшем расширена или адаптирована при появлении новых внешних и внутренних средств защиты ядра ОС семейства Linux.

Методика оценки рисков предполагает практическое ее использование для определения уровня защищенности автоматизированных систем управления технологическими процессами на базе ОС семейства Linux при выявлении необходимости разработки новых или внедрения существующих механизмов защиты в ядро Linux и может быть адаптирована для проведения риск-анализа уязвимостей другого типа при использовании схожей классификации.

Список литературы

1. Демьянович Ю. К., Лебединский Д. М. Операционная система UNIX (LINUX) и распараллеливание; Изд-во Санкт-Петербургского ун-та. М., 2005. 112 с.

2. Terje Aven. Risk assessment and risk management: [Текст] / Terje Aven. // Review of recent advances on their foundation. European Journal of Operational Research. – 16 August 2016. V. 253, Issue 1. P. 1-13.

3. Банк данных угроз безопасности информации ФСТЭК России. URL : https://bdu.fstec.ru/ (дата обращения 30.08.2023).

4. National Vulnerability Database. URL : https://nvd.nist.gov/vuln (дата обращения 30.08.2023).

5. FernandoVano-Garcia. KASLR-MT: Kernel Address Space Layout Randomization for Multi-Tenant cloud systems. [Текст] / FernandoVano-Garcia, Hector Marco-Gisbert. // Journal of Parallel and Distributed Computing. 2022. V. 167. P. 77-90.

6. Выонг, Х.Б. Количественные методы в риск-менеджменте / Х.Б. Выонг // Актуальные вопросы экономических наук. 2016. № 1. С. 42-47.

7. Александровская, Л.Н. Математические основы риск-менеджмента технических систем. / Л.Н. Александровская // Учебное пособие. Том 1: Экспертные методы оценки в риск-менеджменте. М.: Аир, 2017. 834 с.

8. Маховикова, Г.А. Анализ и оценка рисков в бизнесе 2-е изд., пер. и доп. / Г.А. Маховикова. // Учебник и практикум для академического бакалавриата. М.: Юрайт, 2019. 588 с.

Государственный научно- исследовательский испытательный институт проблем технической защиты информации ФСТЭК России
State science research experimental institute of technical information protection problem of Federal service of technical an export control

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 10.09.2023

Информация об авторах

Сердечный Алексей Леонидович – канд. техн. наук, начальник лаборатории, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России, e-mail: alex-voronezh@mail.ru

Каданцев Игорь Александрович – канд. техн. наук, заместитель начальника управления, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России, e-mail: kadanstevigor@mail.ru

Лоскутов Денис Иванович – аспирант, Воронежский Государственный Технический Университет, e-mail: dionisyi99@mail.ru

ASSESSMENT AND REGULATION OF RISKS FOR AUTOMATED SYSTEMS ASSOCIATED WITH THE POSSIBILITY OF PRIVILEGE ESCALATION IN LINUX OPERATING SYSTEMS

A.L. Serdechnyy, I.A. Kadantsev, D.I. Loskutov

In this article the assessment and management of risks for automated systems associated with the possibility of privilege escalation in operating systems of the Linux family were carried out. A classification of vulnerabilities related to privilege escalation in automated systems based on Linux operating systems has been made, taking into account the possibility of quantitatively assessing the risks arising from the exploitation of such vulnerabilities. A method for assessing the risks of the risks under consideration is proposed. This method was developed based on converting the qualitative metrics of the CVSS standard into quantitative metrics aimed at determining the possibility of vulnerability exploitation and the degree of damage to an automated system based on the Linux operating system.

Keywords: Linux operating system, privilege escalation, risk, vulnerability, increased security of an automated system. Suggestions was given for using this technique to assess the risks of exploiting vulnerabilities in more complex data structures.

Submitted 10.09.2023

Information about the authors

Alexey L. Serdechnyy – Cand. Sc. (Technical), Chief of Laboratory, State science research experimental institute of technical information protection problem of Federal service of technical an export control, e-mail: alex-voronezh@mail.ru

Igor A. Kadantsev – Cand. Sc. (Technical), Deputy Head of Department, State science research experimental institute of technical information protection problem of Federal service of technical an export control, e-mail: kadanstevigor@mail.ru

Denis I. Loskutov – Graduate Student, Voronezh State Technical University, e-mail: dionisyi99@mail.ru