УДК 004.056.5

Карасев Е.В.

студент

Поволжский государственный университет

телекоммуникаций и информатики

АНАЛИЗ УЯЗВИМОСТЕЙ ОПЕРАЦИОННОЙ СИСТЕМЫ РЕД ОС

Аннотация

В научной статье рассматриваются уязвимости операционной системы РЕД ОС. Представлены результаты количественного анализа, отражающие соотношение уязвимостей по их степени критичности относительно друг друга. Выявлены наиболее распространенные векторы атаки.

Ключевые слова: уязвимость, операционная система, метод анализа, CVSS, РЕД ОС.

Karasev E.V., Makarov I.S. Analysis of vulnerabilities of the RED OS operating system. The scientific article discusses the vulnerabilities of the RED OS operating system. The results of a quantitative analysis are presented, reflecting the ratio of vulnerabilities according to their degree of criticality relative to each other. The most common attack vectors have been identified. Analysis method, vulnerability, RED OS.

В современном мире невозможно обойтись без электронных вычислительных машин. Они могут быть представлены как компьютерами (далее – ПК), в том числе ноутбуками, так и смартфонами, и планшетами. Для каждого из данных устройств необходимы свои операционные системы. Например, для ПК и ноутбуков зачастую используют операционные системы семейства Microsoft Windows и семейства Linux, для смартфонов и планшетов распространены Android и iOS.

В настоящее время в Российской Федерации существует спрос на отечественное программное обеспечение, и операционные системы не исключение.

Одним из примеров подобной операционной системы является «Ред ОС» разрабатываемый компанией ООО «РЕД СОФТ». Данная операционная система имеет 2 редакции: сертифицированная и стандартная. Стандартная лицензия имеет актуальную версию Linux, регулярные обновления пакетов официального репозитория. Доступна для некоммерческого использования и тестирования компаниями. Сертифицированная версия соответствует всем требованиям Федеральной службы по техническому и экспортному контролю Российской Федерации и включена в реестр программного обеспечения Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

В данной работе используется банк данных угроз безопасности информации ФСТЭК России, в первую очередь для демонстрации количественных значений уязвимостей, связанных с операционной системой «Ред ОС», низкого, среднего, высокого и критического уровня. В выборке находятся 152 уязвимости, обнаруженные за 2024 год и 100 уязвимостей, обнаруженных за 2023 год, каждой из которых присвоен свой уровень опасности. На представленной таблице вы видите число угроз, отнесенных к каждому уровню опасности уязвимости, на основании стандартов CVSS 2.0 и CVSS 3.0 соответственно. Также ФСТЭК России относит уязвимости, набравшие 10 баллов по стандарту CVSS 2.0 к критическим. В данной выборке таковых 19.

Базовая оценка	**Количество**
Низкий уровень (0.0-3.9)	3
Средний уровень (4.0-6.9)	55
Высокий уровень (7.0-10.0) (Из них отнесенных ФСТЭК России к	42 (9)

критическим)	
Итого	100

Таблица 1 – соотношение количества уязвимостей, в зависимости от уровня критичности за 2023 год по стандарту CVSS 2.0.

Базовая оценка	**Количество**
Низкий уровень (0.0-3.9)	2
Средний уровень (4.0-6.9)	54
Высокий уровень (7.0-8.9)	36
Критический уровень (9.0-10.0)	8
Итого	100

Таблица 2 – соотношение количества уязвимостей, в зависимости от уровня критичности за 2023 год по стандарту CVSS 3.0.

Базовая оценка	**Количество**
Низкий уровень (0.0-3.9)	11
Средний уровень (4.0-6.9)	47
Высокий уровень (7.0-10.0) (Из них отнесенных ФСТЭК России к критическим)	94 (47)
Итого	152

Таблица 3 – соотношение количества уязвимостей, в зависимости от уровня критичности за 2024 год по стандарту CVSS 2.0.

Базовая оценка	**Количество**
Низкий уровень (0.0-3.9)	11
Средний уровень (4.0-6.9)	48
Высокий уровень (7.0-8.9)	81
Критический уровень (9.0-10.0)	12
Итого	152

Таблица 4 – соотношение количества уязвимостей, в зависимости от уровня критичности за 2024 год по стандарту CVSS 3.0.

Рассмотрим пример уязвимости, которой присвоен критический уровень уязвимости по обеим версиям стандарта.

– **BDU:2024-02532:** Уязвимость модуля WebAssembly браузера Google Chrome и Microsoft Edge, позволяющая нарушителю выполнить произвольный код.

Тип ошибки: доступ к ресурсу через несовместимые типы.

Класс уязвимости: уязвимость кода.

Расчёт по формуле CVSS 2.0 (базовая оценка):

Способ получения доступа: сетевой, AV = 1.

Сложность получения доступа: низкая, AC = 0,71.

Аутентификация: не требуется, Au = 0,704.

Влияние на конфиденциальность: полное, C = 0,66.

Влияние на целостность: полное, I = 0,66.

Влияние на доступность: полное, A = 0,66.

$$E = 20 * 1 * 0{,}71 * 0{,}704 = 9{,}9968$$

$$Imp = 10{,}41 * (1 – (1 – 0{,}660) * (1 – 0{,}660) * (1 – 0{,}660)) = 10$$

$$f(I)\begin{cases} 0, при\ Imp = 0 \\ 1{,}176, в\ ином\ случае \end{cases}$$

$$BS = ((0{,}6 * 10) + (0{,}4 * 9{,}9968) – 1{,}5) * 1{,}176 = 10$$

Способ эксплуатации уязвимости: подмена при взаимодействии.

Расчёт по формуле CVSS 3.0 (базовая оценка):

Вектор атаки: сетевой, AV = 0,85

Сложность атаки: низкая, AC = 0,77

Уровень привилегий: не требуется, PR = 0,85

Взаимодействие с пользователем: требуется, UI = 0,62

Влияние на другие компоненты системы: оказывает, S = Changed.

Влияние на конфиденциальность: высокое, C = 0,56.

Влияние на целостность: высокое, I = 0,56.

Влияние на доступность: высокое, A = 0,56.

$$E = 8{,}22 * 0{,}85 * 0{,}77 * 0{,}85 * 0{,}62 = 2{,}8$$

$$ISCbase = 1 – ((1 – 0{,}56) * (1 – 0{,}56) * (1 – 0{,}56)) = 0{,}92$$

$$Imp=\begin{cases} 6{,}42*ISCbase\text{, если } S=Unchanged, \\ 7{,}52*(ISCbase-0{,}029)-3{,}25*(ISCbase-0{,}02)^{15}\text{, если } S=Changed. \end{cases}$$

$$Imp = 7{,}52 * (0{,}92 - 0{,}029) - 3{,}25 * (0{,}92 - 0{,}02)^{15} = 6{,}03$$

$$BS=¿$$

$$BS = Roundup\ (1{,}08 * (6{,}03 + 2{,}8)) = 9{,}6$$

Рассмотрев уязвимости, которым присвоен критический уровень опасности по хотя бы одной из версий стандарта CVSS можно сделать следующие выводы:

1. Критический уровень опасности свойственен сторонним приложениям иностранного происхождения.
2. Все уязвимости возможно реализовать удалённо.
3. Все имеют низкий уровень реализации.
4. Только 2 уязвимости из 19 не имеют влияния на конфиденциальность, целостность или доступность, остальные влияют на все 3 показателя в равной мере.

Использованные источники:

1. Официальный сайт РЕД ОС: База знаний / [Электронный ресурс] // РЕД Софт: [сайт]. — URL: https://redos.red-soft.ru/base (дата обращения: 02.05.2024).

2. Банк данных угроз безопасности информации ФСТЭК России / [Электронный ресурс] // ФСТЭК России : [сайт]. — URL: https://bdu.fstec.ru/vul/ (дата обращения: 02.05.2024).