

*Гаврилова П.Н. студентка*

*Российский государственный университет нефти и газа им. И.М. Губкина  
(г. Москва, Россия)*

*Колева М.Ф. студентка*

*Российский государственный университет нефти и газа им. И.М. Губкина  
(г. Москва, Россия)*

## **ПРИМЕНЕНИЕ АКТУАЛЬНЫХ CVE В WINDOWS FIREWALL И ЕГО КОМПОНЕНТАХ**

*Аннотация.* работа анализирует практическое применение уязвимостей (CVE) в Windows Firewall / Microsoft Defender Firewall за 2024–2025 гг. Отобрано пять CVE по классам повышения привилегий, путаницы типов, некорректного контроля доступа и чтения за пределами буфера. Тестирование велось на Windows 11 (24H2, 25H2) и Windows Server (2022, 2025) в виртуальной среде. Результаты подчеркивают необходимость регулярных обновлений для снижения рисков.

*Ключевые слова:* Windows Firewall, Microsoft Defender Firewall, уязвимости, CVE, CWE, безопасность операционных систем, тестирование, обновления безопасности.

Современные операционные системы семейства Microsoft Windows включают встроенные механизмы защиты, обеспечивающие сетевую безопасность и контроль взаимодействия процессов с внешними ресурсами. Центральным элементом данной архитектуры является Windows Firewall (Microsoft Defender Firewall), реализующий фильтрацию сетевого трафика, применение политик безопасности и взаимодействие с компонентами ядра операционной системы. Нарушения в работе данного компонента напрямую отражаются на устойчивости системы к локальным и сетевым атакам.

Анализ данных Microsoft Security Response Center и National Vulnerability Database показывает, что даже в поддерживаемых версиях Windows регулярной выявляются уязвимости, затрагивающие механизмы сетевой фильтрации и контроля доступа. Наибольший практический интерес представляют уязвимости классов повышения привилегий (Elevation of Privilege), путаницы типов (Type Confusion), некорректного контроля доступа (Improper Access

Control) и чтения за пределами буфера (Out-of-bounds Read), поскольку они потенциально позволяют локальному пользователю обходить защитные механизмы или получать доступ к информации, не предусмотренной моделью безопасности.

В рамках настоящей работы использовались сведения из публичных баз данных уязвимостей и официальных бюллетеней безопасности Microsoft. Отбор уязвимостей осуществлялся на основе их актуальности (2024–2025 гг.) и прямой связи с компонентами Windows Firewall и смежными подсистемами. Для анализа CVE применялись методы классификации уязвимостей по CWE, сопоставление с патчами безопасности Microsoft, а также экспериментальное моделирование типовых сценариев возникновения ошибок.

Для практического исследования была сформирована выборка из пяти актуальных CVE, затрагивающих ключевые компоненты сетевой безопасности Windows (табл. 1).

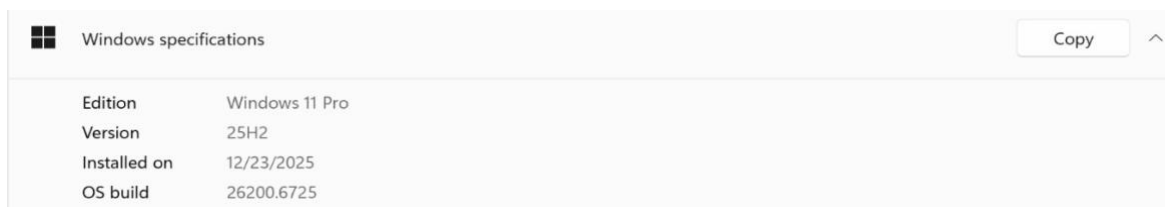
Таблица 1. Выборка исследуемых уязвимостей (CVE)

Идентификатор CVE	Дата публикации	Краткое описание (перевод/адаптация)
<b>CVE-2025-62468</b>	2025-12-09	Чтение за пределами буфера (Out-of-bounds Read) в службе Windows Defender Firewall позволяет авторизованному злоумышленнику локально раскрывать информацию.
<b>CVE-2025-54915</b>	2025-09-09	Доступ к ресурсу с использованием несовместимого типа («путаница типов», Type Confusion) в службе Windows Defender Firewall позволяет авторизованному злоумышленнику локально повысить привилегии.
<b>CVE-2025-54109</b>	2025-09-09	Доступ к ресурсу с использованием несовместимого типа («путаница типов», Type Confusion) в службе Windows Defender Firewall позволяет
		авторизованному злоумышленнику локально повысить привилегии.

<b>CVE-2025-26678</b>	2025-04-08	Некорректный контроль доступа (Improper Access Control) в Windows Defender Application Control (WDAC) позволяет неавторизованному злоумышленнику локально обойти функцию безопасности.
<b>CVE-2024-38034</b>	2024-07-09	Уязвимость повышения привилегий (Elevation of Privilege) в Windows Filtering Platform.

Практическая часть исследования основывалась на анализе механизмов возникновения уязвимостей и сопоставлении поведения системы до и после установки официальных обновлений безопасности Microsoft. Ввиду отсутствия публичных proof-of-concept для большинства рассматриваемых CVE применялся подход экспериментального моделирования, ориентированный на анализ соответствующих классов уязвимостей (CWE) и документированных изменений в логике работы компонентов.

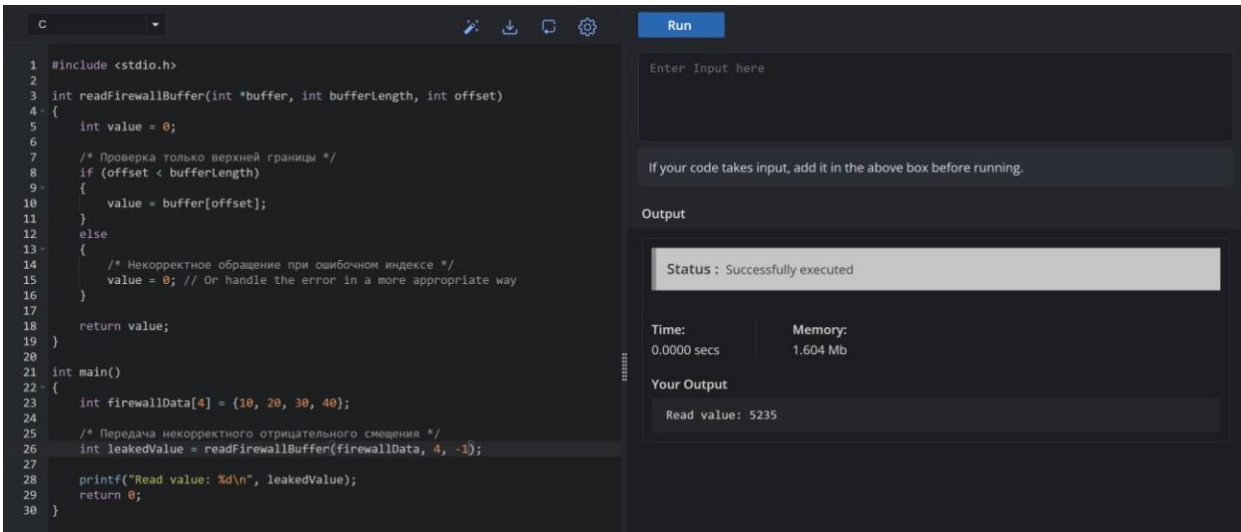
Экспериментальное тестирование проводилось в виртуализированной среде VMware Workstation с использованием операционных систем Windows 11 (сборки 24H2 и 25H2) и Windows Server (2022, 2025), развернутых без установки обновлений безопасности, устраняющих исследуемые уязвимости. Все эксперименты выполнялись под учетной записью с обычными пользовательскими привилегиями, что соответствует заявленным в описаниях CVE условиям эксплуатации. На рисунке 1 представлена информация о версии и сборке тестируемой операционной системы до установки обновлений безопасности.



*Рисунок 1 – Версия и сборка операционной системы Windows до установки обновлений безопасности*

Одной из рассмотренных уязвимостей является CVE-2025-62468, затрагивающая службу Windows Defender Firewall Service и относящаяся к классу CWE-125. Уязвимость позволяет авторизованному локальному пользователю раскрывать информацию вследствие чтения данных за пределами выделенного буфера.

Механизм уязвимости Out-of-bounds Read заключается в неполной проверке границ массива при обращении к памяти: индекс проверяется только по верхней границе, без учета минимально допустимого значения. В результате возможно чтение данных за пределами выделенного буфера. При передаче отрицательного значения смещения происходит чтение данных за пределами выделенного массива (рис. 2). Аналогичный принцип обработки некорректных входных данных может реализовываться и в случае CVE-2025-62468, что приводит к раскрытию информации.



```
1 #include <stdio.h>
2
3 int readFirewallBuffer(int *buffer, int bufferLength, int offset)
4 {
5     int value = 0;
6
7     /* Проверка только верхней границы */
8     if (offset < bufferLength)
9     {
10         value = buffer[offset];
11     }
12     else
13     {
14         /* Некорректное обращение при ошибочном индексе */
15         value = 0; // Or handle the error in a more appropriate way
16     }
17
18     return value;
19 }
20
21 int main()
22 {
23     int firewallData[4] = {10, 20, 30, 40};
24
25     /* Передача некорректного отрицательного смещения */
26     int leakedValue = readFirewallBuffer(firewallData, 4, -1);
27
28     printf("Read value: %d\n", leakedValue);
29     return 0;
30 }
```

Enter Input here

If your code takes input, add it in the above box before running.

Output

Status: Successfully executed

Time: 0.0000 secs      Memory: 1.604 Mb

Your Output

Read value: 5235

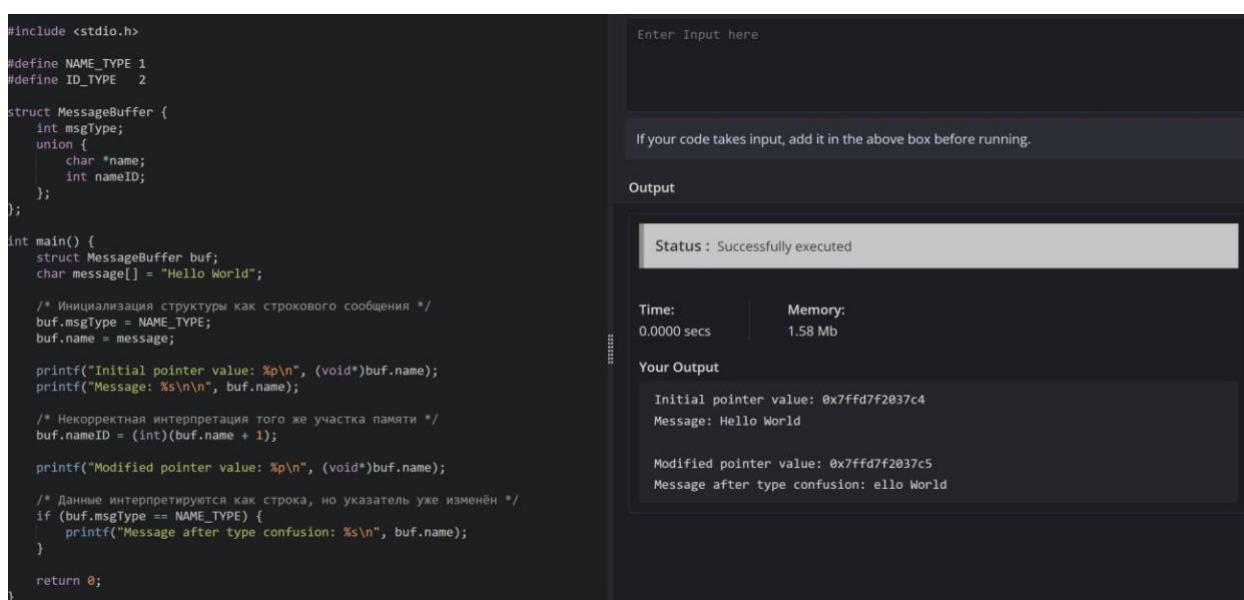
*Рисунок 2 – Демонстрационный код для воспроизведения ошибки чтения за пределами буфера*

Уязвимость CVE-2025-62468 была устранена в рамках официального обновления безопасности Microsoft, опубликованного в декабре 2025 года.

Уязвимости CVE-2025-54915 и CVE-2025-54109 затрагивают службу Windows Defender Firewall Service и относятся к классу CWE-843 (Access of Resource Using Incompatible Type, Type Confusion). Данные уязвимости

позволяют авторизованному локальному пользователю повысить привилегии вследствие некорректной обработки типов данных при доступе к ресурсам.

Механизм уязвимостей класса Type Confusion заключается в использовании одного и того же участка памяти для представления данных различных типов без строгой проверки их актуального состояния. В результате данные интерпретируются в несоответствующем контексте, что может приводить к искажению указателей, обращению к некорректным адресам памяти или нарушению логики управления доступом. В демонстрационном примере на рисунке 3 изменение значения одного поля приводит к непреднамеренному изменению другого, логически несвязанного поля, что иллюстрирует принцип путаницы типов.



```
#include <stdio.h>

#define NAME_TYPE 1
#define ID_TYPE 2

struct MessageBuffer {
    int msgType;
    union {
        char *name;
        int nameID;
    };
};

int main() {
    struct MessageBuffer buf;
    char message[] = "Hello World";

    /* Инициализация структуры как строкового сообщения */
    buf.msgType = NAME_TYPE;
    buf.name = message;

    printf("Initial pointer value: %p\n", (void*)buf.name);
    printf("Message: %s\n\n", buf.name);

    /* Некорректная интерпретация того же участка памяти */
    buf.nameID = (int)(buf.name + 1);

    printf("Modified pointer value: %p\n", (void*)buf.name);

    /* Данные интерпретируются как строка, но указатель уже изменён */
    if (buf.msgType == NAME_TYPE) {
        printf("Message after type confusion: %s\n", buf.name);
    }

    return 0;
}
```

Enter Input here

If your code takes input, add it in the above box before running.

Output

Status: Successfully executed

Time:	Memory:
0.0000 secs	1.58 Mb

Your Output

Initial pointer value: 0x7ffd7f2037c4  
Message: Hello World

Modified pointer value: 0x7ffd7f2037c5  
Message after type confusion: ello World

*Рисунок 3 – Демонстрационный код, иллюстрирующий механизм уязвимости класса Type Confusion*

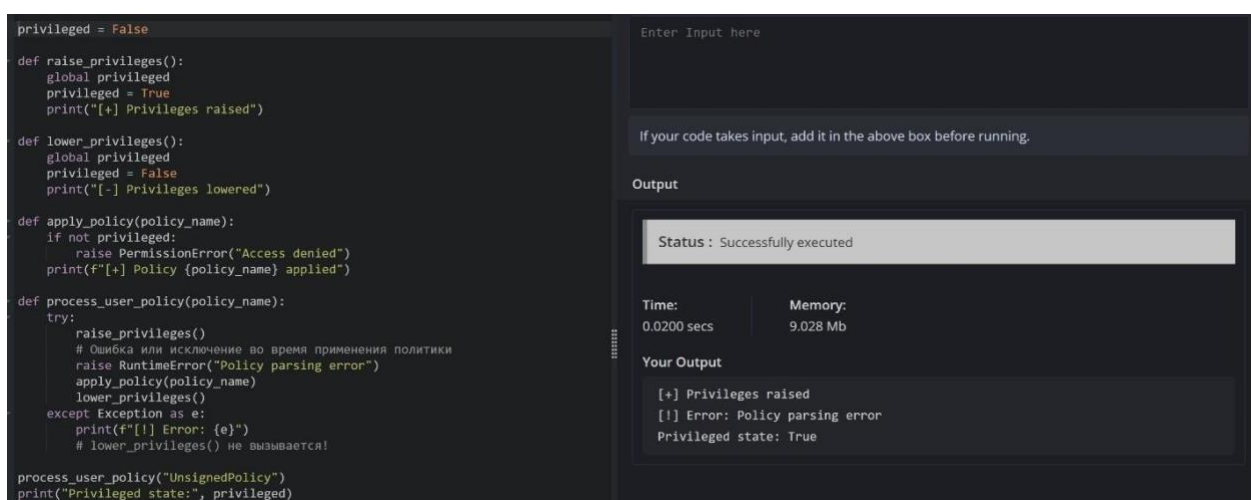
В уязвимостях CVE-2025-54915 и CVE-2025-54109 служба Windows Defender Firewall Service (MpsSvc) некорректно интерпретирует типы внутренних объектов при обработке запросов управления. В результате объект одного типа может быть обработан как объект другого типа, что нарушает логику контроля доступа. Поскольку MpsSvc работает с системными привилегиями и взаимодействует с Windows Filtering Platform, подобная

ошибка может позволить локальному пользователю выполнить операции, выходящие за пределы его прав.

Уязвимости CVE-2025-54915 и CVE-2025-54109 были устранены в рамках официального обновления безопасности Microsoft, опубликованного в сентябре 2025 года.

Уязвимость CVE-2025-26678 затрагивает компонент Windows Defender Application Control (WDAC) и относится к классу CWE-284 (Improper Access Control). Уязвимость позволяет локальному неавторизованному пользователю обойти механизм контроля доступа вследствие некорректного управления контекстом привилегий при применении политик безопасности.

Механизм уязвимости CWE-284 связан с ошибкой логики выполнения: операция, требующая повышенных привилегий, инициируется корректно, однако при возникновении исключения или некорректного сценария возврат к исходному уровню доступа не гарантируется. В результате дальнейшие действия выполняются в более привилегированном контексте, чем предусмотрено моделью безопасности. Аналогичный принцип может реализовываться при обработке политик WDAC, что приводит к обходу ограничений на выполнение кода. Демонстрационный фрагмент представлен на рисунке 4.



```
privileged = False

def raise_privileges():
    global privileged
    privileged = True
    print("[+] Privileges raised")

def lower_privileges():
    global privileged
    privileged = False
    print("[-] Privileges lowered")

def apply_policy(policy_name):
    if not privileged:
        raise PermissionError("Access denied")
    print(f"[+] Policy {policy_name} applied")

def process_user_policy(policy_name):
    try:
        raise_privileges()
        # Ошибка или исключение во время применения политики
        raise RuntimeError("Policy parsing error")
        apply_policy(policy_name)
        lower_privileges()
    except Exception as e:
        print(f"[!] Error: {e}")
        # lower_privileges() не вызывается

process_user_policy("UnsignedPolicy")
print("Privileged state:", privileged)
```

Enter Input here

If your code takes input, add it in the above box before running.

Output

Status : Successfully executed

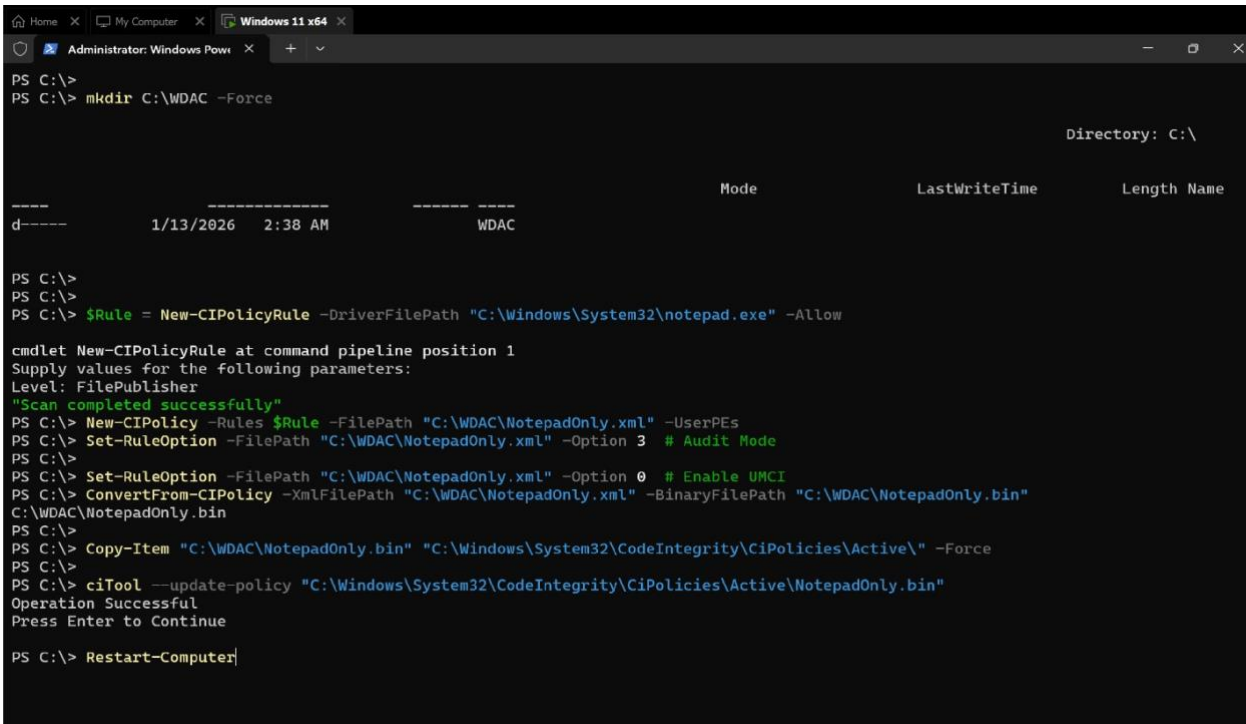
Time: 0.0200 secs      Memory: 9.028 Mb

Your Output

```
[+] Privileges raised
[!] Error: Policy parsing error
Privileged state: True
```

Рисунок 4 – Демонстрационный код, иллюстрирующий ошибку контроля доступа (CWE-284)

Дополнительно на рисунках 5 и 6 показана концепция уязвимости, при которой политики WDAC слишком широки или они не могут проверить целостность файла. Данная схема демонстрирует нарушение модели доступа, лежащее в основе CVE-2025-26678.



```
PS C:\>
PS C:\> mkdir C:\WDAC -Force
PS C:\>

Directory: C:\
-----
Mode                LastWriteTime         Length Name
-----
d-----          1/13/2026   2:38 AM             WDAC

PS C:\>
PS C:\>
PS C:\> $Rule = New-CIPolicyRule -DriverFilePath "C:\Windows\System32\notepad.exe" -Allow

cmdlet New-CIPolicyRule at command pipeline position 1
Supply values for the following parameters:
Level: FilePublisher
"Scan completed successfully"
PS C:\> New-CIPolicy -Rules $Rule -FilePath "C:\WDAC\NotepadOnly.xml" -UserPEs
PS C:\> Set-RuleOption -FilePath "C:\WDAC\NotepadOnly.xml" -Option 3 # Audit Mode
PS C:\>
PS C:\> Set-RuleOption -FilePath "C:\WDAC\NotepadOnly.xml" -Option 0 # Enable UMCI
PS C:\> ConvertFrom-CIPolicy -XmlFilePath "C:\WDAC\NotepadOnly.xml" -BinaryFilePath "C:\WDAC\NotepadOnly.bin"
C:\WDAC\NotepadOnly.bin
PS C:\>
PS C:\> Copy-Item "C:\WDAC\NotepadOnly.bin" "C:\Windows\System32\CodeIntegrity\CiPolicies\Active\" -Force
PS C:\>
PS C:\> ciTool --update-policy "C:\Windows\System32\CodeIntegrity\CiPolicies\Active\NotepadOnly.bin"
Operation Successful
Press Enter to Continue
PS C:\> Restart-Computer|
```

Рисунок 5 – Создание политики WDAC

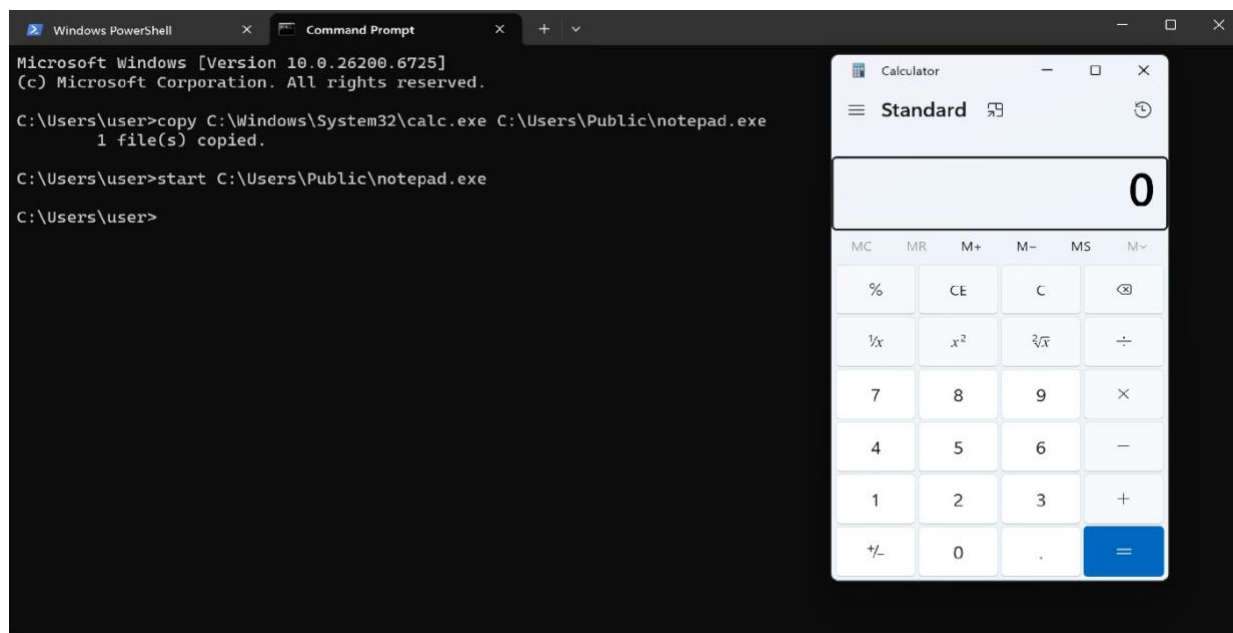


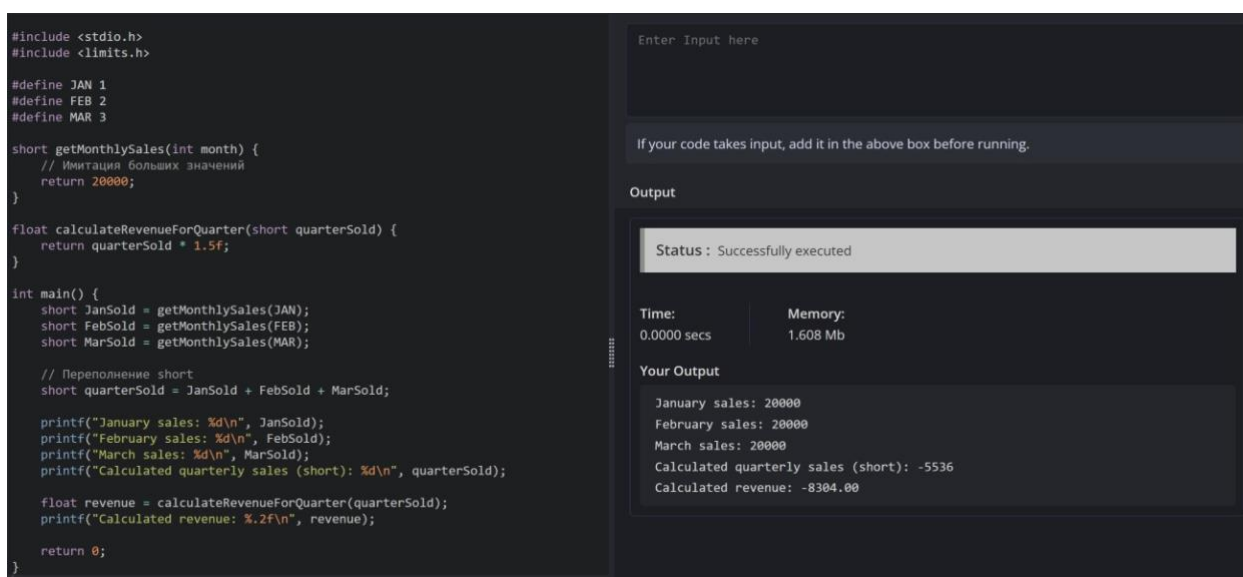
Рисунок 6 – Отсутствие проверки целостности файла

Уязвимость CVE-2025-26678 была устранена в рамках официального обновления безопасности Microsoft, опубликованного в апреле 2025 года, путём корректировки логики управления привилегиями и применения политик Windows Defender Application Control.

Уязвимость CVE-2024-38034 связана с некорректной обработкой целочисленных значений в Windows Filtering Platform и относится к классу CWE-190 (Integer Overflow). При вычислении размера памяти для внутренних структур фильтрации используется значение, которое может переполняться, вследствие чего выделяется меньший объём памяти, чем требуется логике последующей обработки. Это создаёт условия для выхода за пределы выделенной памяти и потенциального повышения привилегий.

Аналогичный механизм может возникать при обработке пользовательских или межпроцессных данных, влияющих на создание и обработку сетевых фильтров в WFP, работающей в привилегированном контексте.

Для демонстрации данного класса уязвимостей используется упрощённый пример на языке C, иллюстрирующий переполнение при вычислении размера памяти для массива структур (рис. 7).



```
#include <stdio.h>
#include <limits.h>

#define JAN 1
#define FEB 2
#define MAR 3

short getMonthlySales(int month) {
    // Имитация больших значений
    return 20000;
}

float calculateRevenueForQuarter(short quarterSold) {
    return quarterSold * 1.5f;
}

int main() {
    short JanSold = getMonthlySales(JAN);
    short FebSold = getMonthlySales(FEB);
    short MarSold = getMonthlySales(MAR);

    // Переполнение short
    short quarterSold = JanSold + FebSold + MarSold;

    printf("January sales: %d\n", JanSold);
    printf("February sales: %d\n", FebSold);
    printf("March sales: %d\n", MarSold);
    printf("Calculated quarterly sales (short): %d\n", quarterSold);

    float revenue = calculateRevenueForQuarter(quarterSold);
    printf("Calculated revenue: %.2f\n", revenue);

    return 0;
}
```

Enter Input here

If your code takes input, add it in the above box before running.

Output

Status : Successfully executed

Time:	Memory:
0.0000 secs	1.608 Mb

Your Output

```
January sales: 20000
February sales: 20000
March sales: 20000
Calculated quarterly sales (short): -5536
Calculated revenue: -8304.00
```

Рисунок 7 – Демонстрационный пример переполнения целочисленного значения (CWE-190)

В данном примере переполнение целочисленного типа short приводит к некорректному вычислению суммарного значения, что нарушает бизнес-логику приложения без явных признаков ошибки выполнения. Аналогичный дефект в компонентах Windows Filtering Platform может быть использован для нарушения целостности памяти в привилегированном коде.

Уязвимость CVE-2024-38034 была устранена в официальном обновлении безопасности Microsoft, опубликованном в июле 2024 года.

В ходе исследования актуальных уязвимостей (CVE) компонентов Windows Firewall и связанных подсистем за 2024–2025 гг. было выявлено, что даже механизмы, изначально предназначенные для усиления безопасности системы, могут содержать логические и реализационные дефекты, потенциально позволяющие локальному пользователю нарушить ограничения доступа или повысить привилегии. Это подтверждает, что наличие встроенных защитных механизмов не гарантирует абсолютной устойчивости системы при отсутствии регулярного обновления и корректной настройки.

Результаты исследования подчеркивают необходимость комплексного подхода к обеспечению безопасности: своевременного применения обновлений безопасности Microsoft, регулярного анализа актуальных CVE, а также тщательной настройки и проверки политик безопасности. Эффективная защита современных операционных систем должна рассматриваться как непрерывный процесс, включающий как технические меры, так и постоянную оценку потенциальных угроз.

## СПИСОК ЛИТЕРАТУРЫ

1. Al-Awadi Yu. M., Baydoun A., Ur Rehman H. Can Windows 11 Stop Well-Known Ransomware Variants? An Examination of Its Built-in Security Features // *Applied Sciences*. – 2024. – Vol. 14, No. 8. – P. 3520. – DOI: 10.3390/app14083520. – (дата обращения: 10.01.2026).

2. CVE.News. Обзоры и аналитика уязвимостей операционных систем [Электронный ресурс]. – URL: <https://www.cve.news> (дата обращения: 10.01.2026).
3. Cyber Press. Windows Defender Firewall Service Vulnerability Lets Attackers Disclose Sensitive Data [Электронный ресурс]. – 10.12.2025. – URL: <https://cyberpress.org/windows-defender-firewall-service-vulnerability/> (дата обращения: 10.01.2026).
4. Microsoft Security Response Center. Руководство по обновлениям безопасности Microsoft [Электронный ресурс]. – URL: <https://msrc.microsoft.com/update-guide/> (дата обращения: 10.01.2026).
5. MITRE Corporation. Common Weakness Enumeration (CWE): каталог типов уязвимостей [Электронный ресурс]. – URL: <https://cwe.mitre.org> (дата обращения: 10.01.2026).
6. National Institute of Standards and Technology. National Vulnerability Database (NVD) [Электронный ресурс]. – URL: <https://nvd.nist.gov> (дата обращения: 10.01.2026).
7. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для СПО / А. Г. Уймин. – 3-е издание, стереотипное. – Санкт-Петербург: Издательство "Лань", 2022. – 480 с. – ISBN 978-5-8114-9255-8.

***Abstract.** The paper considers the practical application and experimental research of recent vulnerabilities (CVE) affecting the components of the Windows Firewall / Microsoft Defender Firewall for the period 2024–2025. As part of the study, five relevant CVEs were selected, belonging to the classes of privilege escalation, type confusion, improper access control, and out-of-bounds read. Experimental testing was conducted on supported versions of the Windows 11 (builds 24H2, 25H2) and Windows Server (2022, 2025) operating systems deployed in a virtual environment. The obtained results demonstrate the necessity of regular operating system updates.*

**Keywords:** *Windows Firewall, Microsoft Defender Firewall, vulnerabilities, CVE, CWE, operating system security, testing, security updates.*