

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО  
ОБРАЗОВАНИЯ  
«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ,  
МЕХАНИКИ И ОПТИКИ»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

**Теория информационной безопасности и методологии защиты информации.**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

**Исследование баз данных угроз и уязвимостей. Калькулятор уязвимостей**

**Выполнил:**

Студент гр. N3249

Шарифуллин Ильдан Айдарович



**Проверил:**

Якимова Софья Андреевна

Санкт-Петербург

2022г.

## Лабораторная работа №1

Исследование баз данных угроз и уязвимостей. Калькулятор уязвимостей

Цель работы: получить знания и навыки работы с различными базами данных угроз и уязвимостей. Работа индивидуальная.

Объекты:


1. Обязательный материал для ознакомления:
  1. <https://habr.com/ru/company/pt/blog/266485/>
  2. <https://habr.com/ru/company/ic-dv/blog/453756/>
  3. <https://xakep.ru/2009/05/15/48221/#toc01>.
  4. <https://habr.com/ru/company/xakep/blog/305262/>
2. БД угроз и уязвимостей (описываем 5 БД и прикладываем пару скриншотов):
  1. ФСТЭК
  2. Vulners
  3. CVE (NVD)
  4. cert/cc
  5. secunia
  6. exploit in
  7. X-Force
  8. SecurityFocus
  9. CNNVD
  10. JVN
  11. <https://www.exploit-db.com>
3. Калькулятор CVSS. Метрики. Выбрать один вариант задачи из каждого блока метрик (задачи а / задачи б и т.д.) и посчитать. (Задачи ниже в текущем документе)

Ход работы:

1. БД угроз и уязвимостей

### 1.1. ФСТЭК

БДУ ФСТЭК – некоторый банк угроз безопасности информации содержащий информацию об основных угрозах и уязвимостях (в первую очередь, характерных для государственных ИС и автоматизированных систем управления производственными и технологическими процессами критически важных объектов). Для каждой угрозы даны описание, источники, объект воздействия и последствия реализации угрозы.



Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю  
ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации  
ФАУ «ТНИИИ ПТЗИ ФСТЭК России»

Угрозы Уязвимости Документы Термины Обратная связь Обновления Участники Обучение ФСТЭК России

Поиск

Главная / Список угроз

ФИЛЬТРАЦИЯ

Контекстный поиск по названию угрозы

Источники угрозы

Доступен множественный выбор

Последствия реализации угрозы:

Нарушение конфиденциальности

Нарушение целостности

Нарушение доступности

Сброс Применить

Выводить по: 10, 20, 50, 100

Элементы с 1 по 10 из 222

- УБИ. 001 Угроза автоматического распространения вредоносного кода в грид-системе
- УБИ. 002 Угроза агрегирования данных, передаваемых в грид-системе
- УБИ. 003 Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации
- УБИ. 004 Угроза аппаратного сброса пароля BIOS
- УБИ. 005 Угроза внедрения вредоносного кода в BIOS
- УБИ. 006 Угроза внедрения кода или данных
- УБИ. 007 Угроза воздействия на программы с высокими привилегиями
- УБИ. 008 Угроза восстановления и/или повторного использования аутентификационной информации

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

16.12.2020 УБИ. 222 Угроза подмены модели машинного обучения

16.12.2020 УБИ. 221 Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных

16.12.2020 УБИ. 220 Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта

16.12.2020 УБИ. 219 Угроза хищения обучающих данных

16.12.2020 УБИ. 218 Угроза раскрытия информации о модели машинного обучения

11.02.2020 УБИ. 217 Угроза использования скомпрометированного доверенного источника

УБИ.183: Угроза перехвата управления автоматизированной системой управления технологическими процессами

Вид

**Описание угрозы**

Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационной инфраструктуре за счёт получения нарушителем права управления входящей в её состав автоматизированной системой управления технологическими процессами путём эксплуатации уязвимостей её программного обеспечения или слабостей технологических протоколов передачи данных. Данная угроза обусловлена наличием у автоматизированной системы управления технологическими процессами программных сетевых интерфейсов взаимодействия и, как следствие, возможностью несанкционированного доступа к данной системе, а также недостаточностью мер фильтрации сетевого трафика и антивирусной защиты. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с автоматизированной системой управления технологическими процессами. Реализация данной угрозы может привести к: блокированию или искажению (некорректность выполнения) алгоритмов отработки заданий управления технологическими процессами, непосредственного управления оборудованием предприятия; нарушению штатного хода технологических процессов; частичному или полному останову технологических процессов без (или с выхода(-ом) оборудования из строя; аварийной ситуации в критической системе информационной инфраструктуры

**Источники угрозы**

Внутренний нарушитель со средним потенциалом

Внешний нарушитель с высоким потенциалом

**Объект воздействия**

Программное обеспечение автоматизированной системы управления технологическими процессами

**Последствия реализации угрозы**

Нарушение целостности

Нарушение доступности

1.2. SecurityFocus

SecurityFocus – новостной и информационный портал об ИБ. Это скорее форум, где люди обменивались различными появившимися угрозами и мнениями, по поводу них. Это не полноценная БДУ. На данный момент ресурс не функционирует, последняя новость была добавлена 16 января 2021 года.

### [SECURITY] [DSA 4624-1] evince security update

FRIDAY, FEBRUARY 14, 2020 09:00 PM | CARNIL DEBIAN ORG 0 replies

-----BEGIN PGP SIGNED MESSAGE-----

[READ MORE](#) →

### CVE-2020-0728: Windows Modules Installer Service Information Disclosure Vulnerability

FRIDAY, FEBRUARY 14, 2020 08:05 PM | RADIMREB3 GMAIL COM 0 replies

The TrustedInstaller service running on the Windows operating system

[READ MORE](#) →

### [TZO-15-2020] - F-SECURE Generic Malformed Container bypass (RAR)

FRIDAY, FEBRUARY 14, 2020 12:59 PM | THIERRY ZOLLER LU 0 replies

[READ MORE](#) →

## [TZO-15-2020] - F-SECURE Generic Malformed Container bypass (RAR)

FRIDAY, FEBRUARY 14, 2020 12:59 PM | THIERRY ZOLLER LU

From the low-hanging-fruit-department  
F-SECURE Generic Malformed Container bypass (RAR)

Ref : [TZO-15-2020] - F-SECURE Generic Malformed Container bypass (RAR)  
Vendor : F-SECURE  
Status : Patched  
CVE : none provided  
Blog : <https://blog.zoller.lu/p/tzo-15-2020-f-secure-generic-malformed.html>  
Vulnerability Disclosure Policy: <https://caravelahq.com/b/policy/20949>

Affected Products  
=====

F-Secure Email and Server Security
F-Secure Internet GateKeeper
F-SECURE CLOUD PROTECTION FOR SALESFORCE

Linux below 17.0.605.474

I. Background

Quote: "Unprecedented challenges threaten to undermine the very survival of society. Only

### 1.3. X-Force

На данный момент БД X-Force по адресу <http://xforce.iss.net/> недоступна. По описанию из разных источников:

поиск уязвимостей в базе данных может быть выполнен по нескольким параметрам:


- по операционной системе или платформе, подверженной уязвимости;
- по имени уязвимости;
- по дате обнаружения;
- по степени риска (высокая, средняя, низкая).

Также существует возможность вывода всех уязвимостей за последний, предпоследний или несколько предыдущих месяцев. Все обнаруженные уязвимости сразу же заносятся в базы данных уязвимостей системы анализа защищенности сетевых сервисов и протоколов Internet Scanner, системы обнаружения атак RealSecure, систем анализа защищенности операционных систем System Scanner и системы анализа защищенности баз данных Database Scanner.




## 1.4. Vulners

БД Vulners содержит огромную базу уязвимостей с оценкой по CVSS и CVSS3. Однако здесь нет строгого фильтра по различным параметрам угрозы. Эта БД предназначена скорее для поиска угроз для конкретных семейств программ (что сильно ее отличает от того же ФСТЭК). В Vulners добавляются общие описания уязвимости и других исследовательских центров и центров реагирования: Vulnerability Lab, XSSed, CERT, ICS, Zero Day Initiative, Positive Technologies, ERPSan.



Microsoft and Other Major Software Firms Release February 2022 Patch Updates  
2022-02-09 06:40:00



cvss 7.6  
cvss3 7.8  
0.9

ID THN:A19D66C10E6D6239DFCE7CD41A974F09

Type thn

Reporter The Hacker News

Modified 2022-02-09 06:40:43

CVSS v3 ▾

Attack Complexity: LOW

Confidentiality Impact: HIGH

Attack Vector: LOCAL

Integrity Impact: HIGH

Privileges Required: LOW

Availability Impact: HIGH

Scope: UNCHANGED

AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Description



## 1.5. CVE (NVD)

NVD – это хранилище данных управления уязвимостями на основе стандартов правительства США, представленное с использованием протокола автоматизации контента безопасности (SCAP).

Эти данные позволяют автоматизировать управление уязвимостями, измерение безопасности и соответствие требованиям.

NVD включает в себя базы данных контрольных списков безопасности, недостатки программного обеспечения, связанные с безопасностью, неправильные конфигурации, названия продуктов и показатели воздействия.

## VULNERABILITIES

## CVE-2022-21687 Detail

## Current Description

gh-ost is a triggerless online schema migration solution for MySQL. Versions prior to 1.1.3 are subject to an arbitrary file read vulnerability. The attacker must have access to the target host or trick an administrator into executing a malicious gh-ost command on a host running gh-ost, plus network access from host running gh-ost to the attack's malicious MySQL server. The `--database` parameter does not properly sanitize user input which can lead to arbitrary file reads.

[View Analysis Description](#)

## Severity

CVSS Version 3.x

CVSS Version 2.0

## CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 6.5 MEDIUM

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N



CNA: GitHub, Inc.

Base Score: 6.5 MEDIUM

Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N

## QUICK INFO

## CVE Dictionary Entry:

CVE-2022-21687

## NVD Published Date:

02/01/2022

## NVD Last Modified:

02/04/2022

## Source:

GitHub, Inc.

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

## VULNERABILITIES

## February 2022

Below is a list of CVEs for the selected month.

**NOTE:** The CVEs shown below have a **release date** in the year and month chosen. The CVE ID may show a year value that does not match the release date, however, the release date will fall within the chosen year and month.

471 entries found for February 2022

CVE-2021-3534	CVE-2022-23774	CVE-2020-8562	CVE-2022-0419	CVE-2022-23602	CVE-2022-23603
CVE-2022-23607	CVE-2021-41040	CVE-2021-43859	CVE-2022-21687	CVE-2022-23596	CVE-2022-23597
CVE-2021-24648	CVE-2021-24686	CVE-2021-24707	CVE-2021-24761	CVE-2021-24762	CVE-2021-24763
CVE-2021-24764	CVE-2021-24765	CVE-2021-24775	CVE-2021-24814	CVE-2021-24868	CVE-2021-24900
CVE-2021-24919	CVE-2021-24926	CVE-2021-24934	CVE-2021-24937	CVE-2021-24944	CVE-2021-24975
CVE-2021-24983	CVE-2021-25063	CVE-2021-25072	CVE-2021-25085	CVE-2021-25089	CVE-2021-25091
CVE-2021-25092	CVE-2021-25093	CVE-2021-25097	CVE-2021-41571	CVE-2021-43848	CVE-2021-45416
CVE-2021-46253	CVE-2022-0220	CVE-2022-0320	CVE-2022-0401	CVE-2022-0417	CVE-2022-23601

## 2. Расчеты по калькулятору CVSS

## 2.1. Оцените уязвимости по базовым метрикам для ситуации при следующих условиях:

е) атака высокой сложности будет проводиться на сетевой уровень системы, при этом не оказывается влияние на другие компоненты системы. Атака приводит к нарушению конфиденциальности и целостности высокого уровня, доступности низкого уровня. При этом требуется взаимодействие с пользователем, уровень привилегий - низкий.

Базовые метрики	6.7	AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N
Базовая оценка (BS): 6.7		
Вектор атаки (AV):		
Сетевой (N)	Смежная сеть (A)	Локальный (L)
Физический (P)		
Сложность атаки (AC):		
Высокая (H)	Низкая (L)	
Уровень привилегий (PR):		
Высокий (H)	Низкий (L)	Не требуется (N)
Взаимодействие с пользователем (UI):		
Требуется (R)	Не требуется (N)	
Влияние на другие компоненты системы (S):		
Не оказывает (U)	Оказывает (C)	
Влияние на конфиденциальность (C):		
Не оказывает (N)	Низкое (L)	Высокое (H)
Влияние на целостность (I):		
Не оказывает (N)	Низкое (L)	Высокое (H)
Влияние на доступность (A):		
Не оказывает (N)	Низкое (L)	Высокое (H)

е) Предполагается, что есть сценарий для средств эксплуатации, есть рекомендации для средств устранения, а информация об уязвимостях получена из достоверных отчетов.

Временные метрики <span>6.1</span>				
Временная оценка (TS): 6.1				
Доступность средств эксплуатации (E):				
Не определено (X)	Высокая (H)	Есть сценарий (F)	Есть PoC-код (P)	Теоретически (U)
Доступность средств устранения (RL):				
Не определено (X)	Недоступно (U)	Рекомендации (W)	Временное (T)	Официальное (O)
Степень доверия к информации об уязвимости (RC):				
Не определено (X)	Подтверждена (C)	Достоверные отчеты (R)	Отчеты (U)	

е) К уровню обеспечения КИД заданы высокие требования, однако влияние оказывается низким. При этом проводится атака неопределенной сложности на сетевой уровень системы. Уровень привилегий в данном случае - низкий, взаимодействия с пользователем не происходит. Также оказывается влияние на другие компоненты системы.

Контекстные метрики <span>6.7</span>				CR HIR HIR HMV NMPR LMI LMI NMS CMC LMI LMI L							
Контекстная оценка (ES): 6.7											
Требования к конфиденциальности (CR):											
Не определено (X)	Низкие (L)	Средние (M)	Высокие (H)	Не определено (X)	Сетевой (N)	Смежная сеть (A)	Локальный (L)	Физический (P)			
Требования к целостности (IR):											
Не определено (X)	Низкие (L)	Средние (M)	Высокие (H)	Не определено (X)	Высокая (H)		Низкая (L)				
Требования к доступности (AR):											
Не определено (X)	Низкие (L)	Средние (M)	Высокие (H)	Не определено (X)	Высокий (H)	Низкий (L)	Не требуется (N)				
Вектор атаки (корп.) (MAV):											
Не определено (X)	Не определено (X)	Требуется (R)	Не требуется (N)	Не определено (X)	Требуется (R)	Не требуется (N)	Не требуется (N)				
Сложность атаки (корп.) (MAC):											
Не определено (X)	Не определено (X)	Требуется (R)	Не требуется (N)	Не определено (X)	Требуется (R)	Не требуется (N)	Не требуется (N)				
Уровень привилегий (корп.) (MPR):											
Не определено (X)	Не определено (X)	Требуется (R)	Не требуется (N)	Не определено (X)	Требуется (R)	Не требуется (N)	Не требуется (N)				
Взаимодействие с пользователем (корп.) (MUI):											
Не определено (X)	Не определено (X)	Требуется (R)	Не требуется (N)	Не определено (X)	Требуется (R)	Не требуется (N)	Не требуется (N)				
Влияние на другие компоненты системы (корп.) (MS):											
Не определено (X)	Не определено (X)	Требуется (R)	Не требуется (N)	Не определено (X)	Требуется (R)	Не требуется (N)	Не требуется (N)				
Влияние на конфиденциальность (корп.) (MC):											
Не определено (X)	Не определено (X)	Требуется (R)	Не требуется (N)	Не определено (X)	Требуется (R)	Не требуется (N)	Не требуется (N)				
Влияние на целостность (корп.) (MI):											
Не определено (X)	Не определено (X)	Требуется (R)	Не требуется (N)	Не определено (X)	Требуется (R)	Не требуется (N)	Не требуется (N)				
Влияние на доступность (корп.) (MA):											
Не определено (X)	Не определено (X)	Требуется (R)	Не требуется (N)	Не определено (X)	Требуется (R)	Не требуется (N)	Не требуется (N)				

**Вывод:** в ходе лабораторной работы я изучил некоторые БД угроз, и определил, для чего я могу их использовать (например: ФСТЭК – угрозы, характерные для гос. ИС, имеют более общее описание, а Vulners – угрозы различных ПО, имеющие конкретные оценки и описания). Далее для разных сценариев я с помощью калькулятора CVSS посчитал базовые, временные и контекстные метрики, показатели которых (для моего сценария) оказались относительно высокими, а значит данные сценарии требовали относительно быстрого реагирования на эти уязвимости.