

## Задание:

Установите сканер уязвимостей и выполните следующие задачи:

1. Проведите сканирование хоста или сети на наличие уязвимостей.
2. Проанализируйте любую критическую уязвимость. Если критическая уязвимость отсутствует, то возьмите следующую по критичности.

Проанализируйте уязвимость на эти критерии:

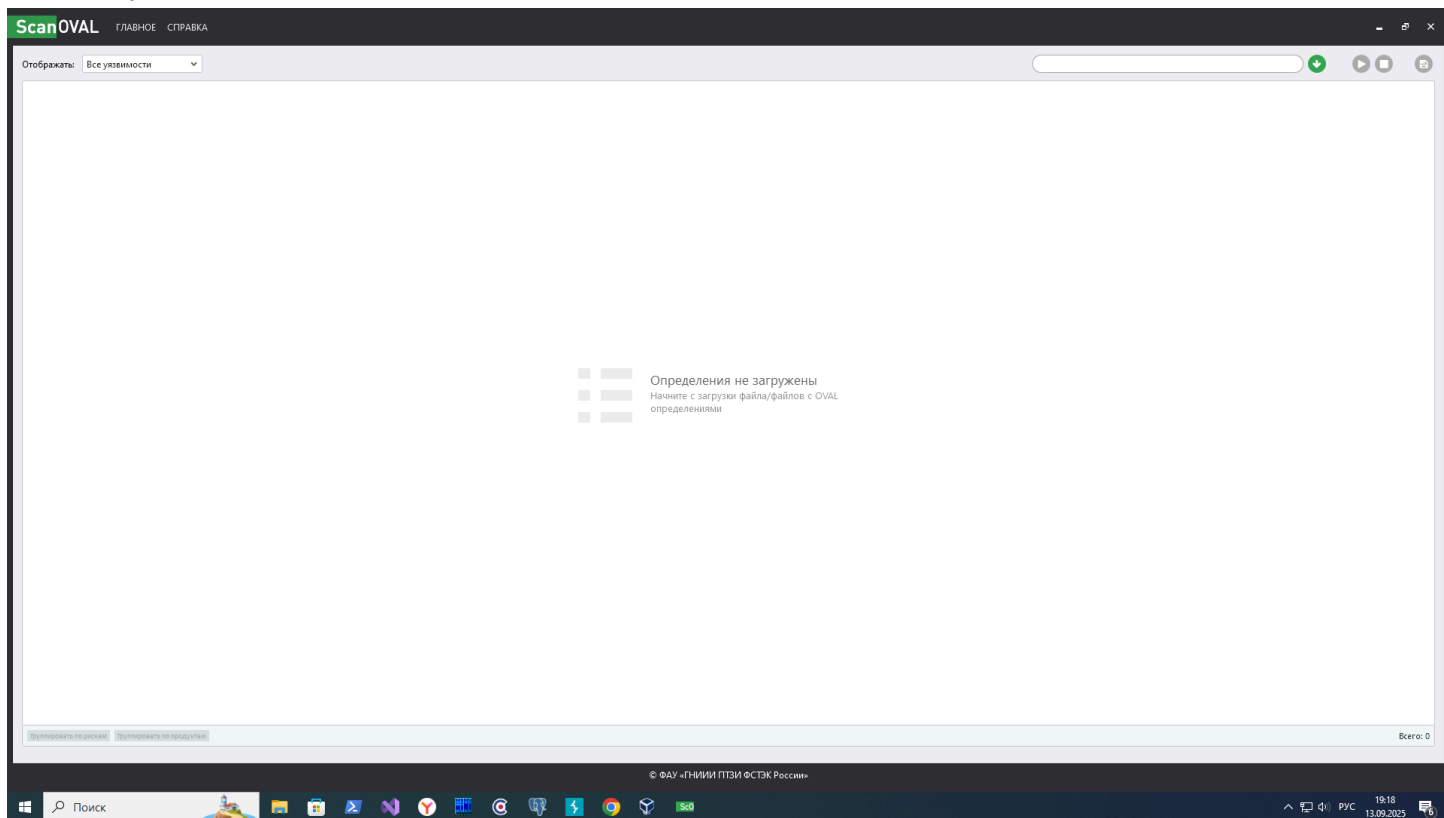
- Что уязвимо?
- Как может быть реализована уязвимость?
- Прочитать описание на CVE?
- Как устранить уязвимость?

3. Устраните уязвимости.

4. Проведите повторное сканирование.

Я буду использовать сканер ScanOVAL.

Запускаю сканер ScanOVAL:



Загружаю базу OVAL определений

ScanOVAL

ГЛАВНОЕ Справка

2 файла(ов) загружено.

Отображать: Все уязвимости

Идентификатор уязвимости	Результат	Уровень	Ссылки на источники	Название уязвимости
BDU-2015-10240	Критический	Уязвимость системы управления базами данных Линтер Бастион, позволяющая злоумышленнику выполнить произвольный код с правами системы (BDU-2015-10240)		
BDU-2021-06345	Критический	VULN-20211124.5; active-saltstack		
BDU-2023-06017	Критический	CVE-2023-5074		
BDU-2021-04041	Критический	mfsa2016-86; mfsa2016-88; CVE-2016-86; CVE-2016-88		
BDU-2023-06077	Критический	CVE-2023-5166		
BDU-2020-02500	Критический	VULN-20200513.14; CVE-2020-090		
BDU-2016-02178	Критический	CVE-2016-4276; arps16-29		
BDU-2022-01702	Критический	CVE-2022-23852; Nessus; Nessus; I		
BDU-2023-08257	Критический	CVE-2023-44446		
BDU-2015-12022	Критический	CVE-2015-7663; arps15-28		
BDU-2015-11675	Критический	230915		
BDU-2022-02541	Критический	PHP_5_5; PHP_5_6; CVE-2016-5770		
BDU-2022-02547	Критический	PHP_7_1; PHP_7_0; CVE-2016-5095		
BDU-2023-06465	Критический	CVE-2023-44160		
BDU-2015-09525	Критический	openssl-dos.txt; 4773; CVE-2006-4		
BDU-2023-06603	Критический	CVE-2023-41419		
BDU-2016-00270	Критический	CVE-2015-6765; stable-channel-up		
BDU-2024-00321	Критический	CVE-2024-22051; GHSA-fm44-26d3-		
BDU-2015-12230	Критический	CVE-2015-8045; arps15-32		
BDU-2022-02555	Критический	PHP_7_0; PHP_5_5; PHP_5_6; CVE-2		
BDU-2024-05906	Критический	VULN-20240729.15; Chr-2024-7-23		
BDU-2016-01366	Критический	PHP_5_6; PHP_5_5; PHP_5_4; CVE-2		
BDU-2016-02310	Критический	CVE-2016-6941; arps16-33		
BDU-2016-01369	Критический	PHP_5_6; PHP_5_5; PHP_5_4; CVE-2		
BDU-2016-02309	Критический	CVE-2016-6942; arps16-33		
BDU-2016-02292	Критический	CVE-2016-6959; arps16-33		
BDU-2017-00034; BDU-2017-0002	Критический	CVE-2016-7879; arps16-39		
BDU-2017-00027; BDU-2016-0233	Критический	CVE-2016-7872; arps16-39		
BDU-2017-00027; BDU-2016-0233	Критический	CVE-2016-7872; arps16-39		
BDU-2021-04796	Критический	VULN-20210914.1; VULN-20210917		
BDU-2025-03316	Критический	VULN-20250303.10; CVE-2025-099		
BDU-2016-00543	Критический	openssl/origin; CVE-2016-1906;		
BDU-2021-04899	Критический	VULN-20211001.3; Chrome-VB-Log		
BDU-2021-05503	Критический	VULN-20211102.3; CVE-2021-3799		
BDU-2021-05969	Критический	VMware-vCenter-Server-Unauth		
BDU-2021-05969	Критический	VMware-vCenter-Server-Unauth		
BDU-2025-02676	Критический	VULN-20250317.81; CVE-2025-191		
BDU-2015-11880	Критический	CVE-2015-4844; openssl2015-33678		

Всего: 32252

© ФАУ «ГНИИИ ПТЭИ ФСТЭК России»

## Запускаю сканирование хостовой машины с помощью ScanOVAL

ScanOVAL

ГЛАВНОЕ Справка

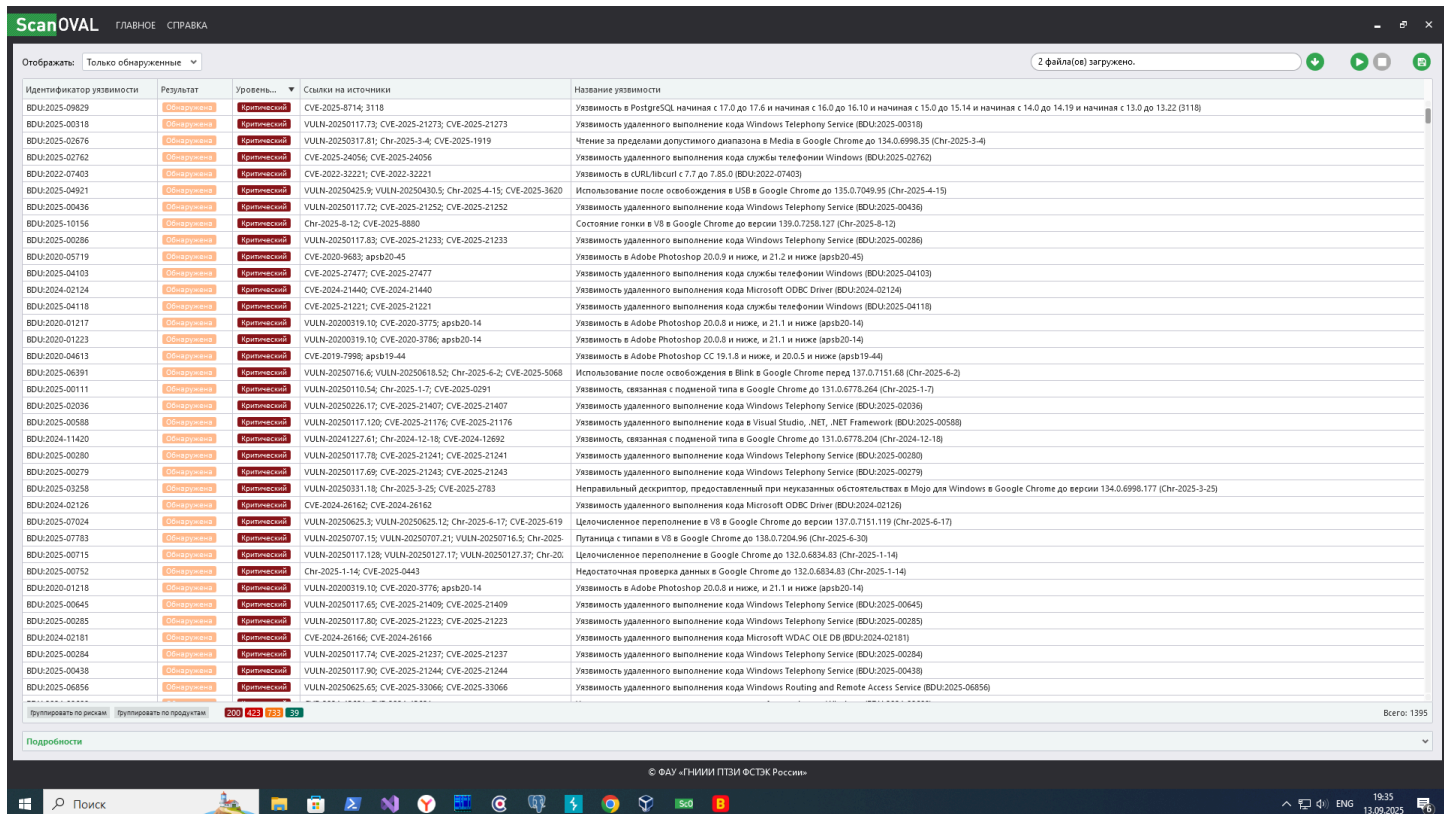
2 файла(ов) загружено.

Отображать: Все уязвимости

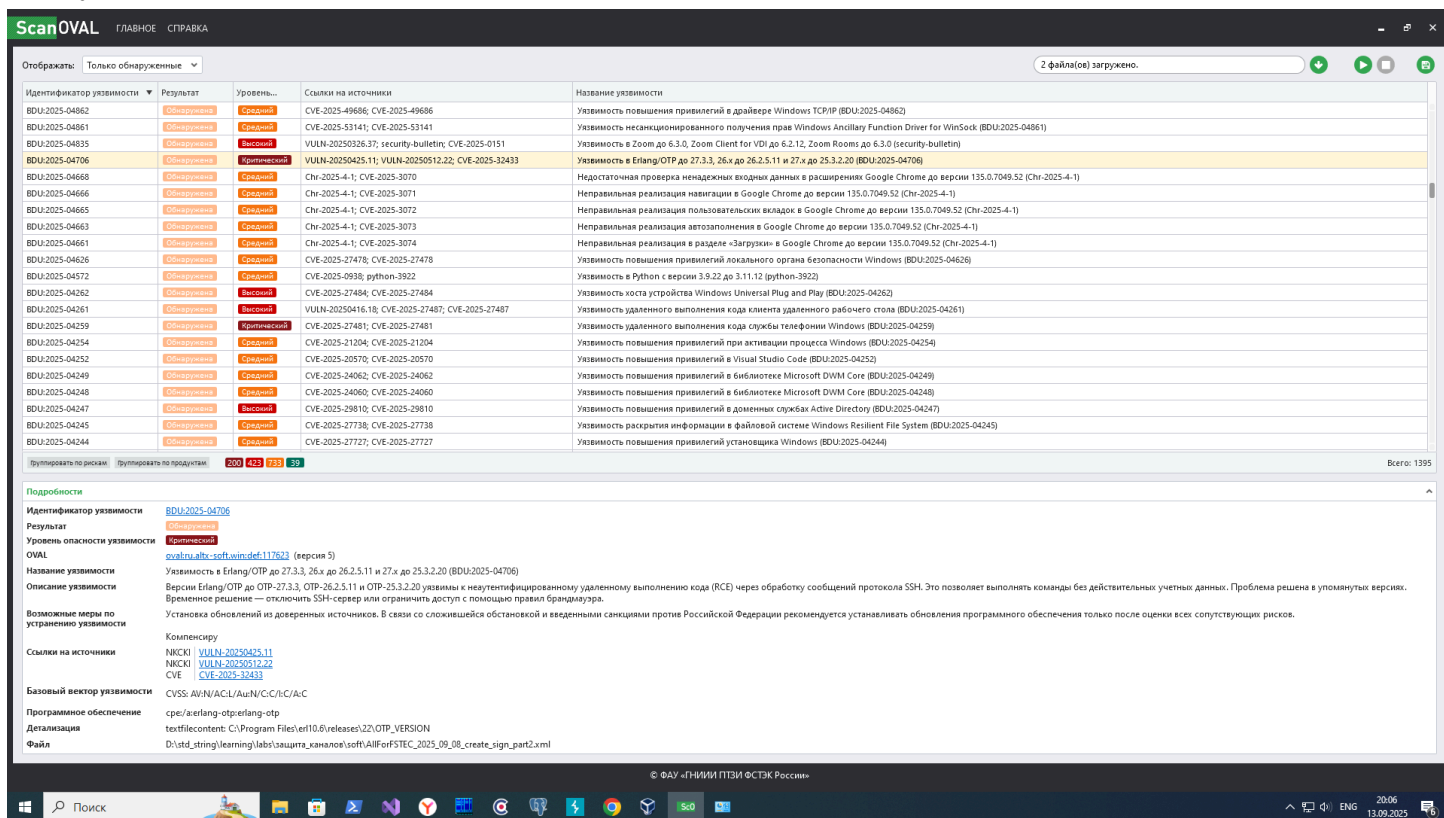
Идентификатор уязвимости	Результат	Уровень	Ссылки на источники	Название уязвимости
BDU-2015-10240	Критический	Уязвимость системы управления базами данных Линтер Бастион, позволяющая злоумышленнику выполнить произвольный код с правами системы (BDU-2015-10240)		
BDU-2021-06345	Критический	VULN-20211124.5; active-saltstack		
BDU-2023-06017	Критический	CVE-2023-5074		
BDU-2021-04041	Критический	mfsa2016-86; mfsa2016-88; CVE-2016-86; CVE-2016-88		
BDU-2023-06077	Критический	CVE-2023-5166		
BDU-2020-02500	Критический	VULN-20200513.14; CVE-2020-090		
BDU-2016-02178	Критический	CVE-2016-4276; arps16-29		
BDU-2022-01702	Критический	CVE-2022-23852; Nessus; Nessus; I		
BDU-2023-08257	Критический	CVE-2023-44446		
BDU-2015-12022	Критический	CVE-2015-7663; arps15-28		
BDU-2015-11675	Критический	230915		
BDU-2022-02541	Критический	PHP_5_5; PHP_5_6; CVE-2016-5770		
BDU-2022-02547	Критический	PHP_7_1; PHP_7_0; CVE-2016-5095		
BDU-2023-06465	Критический	CVE-2023-44160		
BDU-2015-09525	Критический	openssl-dos.txt; 4773; CVE-2006-4		
BDU-2023-06603	Критический	CVE-2023-41419		
BDU-2016-00270	Критический	CVE-2015-6765; stable-channel-up		
BDU-2024-00321	Критический	CVE-2024-22051; GHSA-fm44-26d3-		
BDU-2015-12230	Критический	CVE-2015-8045; arps15-32		
BDU-2022-02555	Критический	PHP_7_0; PHP_5_5; PHP_5_6; CVE-2		
BDU-2024-05906	Критический	VULN-20240729.15; Chr-2024-7-23		
BDU-2016-01366	Критический	PHP_5_6; PHP_5_5; PHP_5_4; CVE-2		
BDU-2016-02310	Критический	CVE-2016-6941; arps16-33		
BDU-2016-01369	Критический	PHP_5_6; PHP_5_5; PHP_5_4; CVE-2		
BDU-2016-02309	Критический	CVE-2016-6942; arps16-33		
BDU-2016-02292	Критический	CVE-2016-6959; arps16-33		
BDU-2017-00034; BDU-2017-0002	Критический	CVE-2016-7879; arps16-39		
BDU-2017-00027; BDU-2016-0233	Критический	CVE-2016-7872; arps16-39		
BDU-2017-00027; BDU-2016-0233	Критический	CVE-2016-7872; arps16-39		
BDU-2021-04796	Критический	VULN-20210914.1; VULN-20210917		
BDU-2025-03316	Критический	VULN-20250303.10; CVE-2025-099		
BDU-2016-00543	Критический	openssl/origin; CVE-2016-1906;		
BDU-2021-04899	Критический	VULN-20211001.3; Chrome-VB-Log		
BDU-2021-05503	Критический	VULN-20211102.3; CVE-2021-3799		
BDU-2021-05969	Критический	VMware-vCenter-Server-Unauth		
BDU-2021-05969	Критический	VMware-vCenter-Server-Unauth		
BDU-2025-02676	Критический	VULN-20250317.81; CVE-2025-191		
BDU-2015-11880	Критический	CVE-2015-4844; openssl2015-33678		

Всего: 32252

© ФАУ «ГНИИИ ПТЭИ ФСТЭК России»



Выбираю одну критическую уязвимость. В качестве такой уязвимости я беру уязвимость BDU:2025-04706 (CVE-2025-32433)



Вот описание этой уязвимости на сайте ФСТЭК:

Bank of threat data for information security

Федеральная служба по техническому и экспортному контролю  
ФСТЭК России

Государственный научно-исследовательский испытательный институт  
проблем технической защиты информации  
ФАН «ГНИИИ ПТЗИ ФСТЭК России»

Угрозы - Уязвимости - Тестирование обновлений - Документы - Обратная связь - Обновления - Участники - Обучение - БДУ АСУ ТП - ФСТЭК России

Главная / Список уязвимостей / BDU:2025-04706

Вид

Описание уязвимости: Уязвимость реализации протокола SSH из набора библиотек Erlang/OTP связана с отсутствием проверки подлинности для критически важной функции. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированных SSH-пакетов

Уязвимое ПО	Вендор	Наименование ПО	Версия ПО	Тип ПО
	ООО «Ред Софт»	РЕД ОС (запись в едином реестре российских программ №3751)	7.3	Операционная система
	ООО «РусБИТех-Астра»	Astra Linux Special Edition (запись в едином реестре российских программ №369)	1.7	Операционная система
	ООО «РусБИТех-Астра»	Astra Linux Special Edition (запись в едином реестре российских программ №369)	1.8	Операционная система
Сообщество свободного программного обеспечения	Erlang/OTP		до 27.3.3	Микропрограммный код
Сообщество свободного программного обеспечения	Erlang/OTP		до 26.2.5.11	Микропрограммный код
Сообщество свободного программного обеспечения	Erlang/OTP		до 25.3.2.20	Микропрограммный код
Cisco Systems Inc.	ConfD		до 7.7.19.1	Сетевое средство Сетевое программное средство
Cisco Systems Inc.	ConfD		до 8.1.16.2	Сетевое средство Сетевое программное

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

13.09.2025  
Уязвимость реализации протокола Address Resolution Protocol (ARP) операционной системы Cisco IOS XR, позволяющая нарушителю вызвать отказ в обслуживании

13.09.2025  
Уязвимость интеграционной IoT/SCADA платформы Delta Industrial Automation DIALink, связанная с неверным ограничением имени пути к каталогу с ограниченным доступом, позволяющая нарушителю выполнить произвольный код

12.09.2025  
Уязвимость службы Defender Firewall Service операционных систем Windows, позволяющая нарушителю повысить свои привилегии

12.09.2025  
Уязвимость класса MarControl операционных систем Windows, позволяющая нарушителю повысить свои привилегии

12.09.2025  
Уязвимость программы для просмотра электронных документов в стандарте PDF Foxit PDF Reader (pawee Foxit Reader), связанная с доступом к неинициализированному указателю, позволяющая нарушителю выполнить произвольный код или повредить память

12.09.2025  
Уязвимость компонента Broker VM платформы безопасности Cortex XDR, связанная с использованием учетных данных по умолчанию, позволяющая нарушителю получить доступ к внутренним службам на других виртуальных машинах

12.09.2025  
Уязвимость обработки файлов Terraform инструмента для статического анализа кода Checkov by Datascope

19:51  
13.09.2025

Вот описание этой уязвимости на cve.org:

CVE 25 YEARS

About Partner Information Program Organization Downloads Resources & Support Report/Request

### CNA: GitHub (maintainer security advisories)

Published: 2025-04-16 Updated: 2025-04-16  
Title: Erlang/OTP SSH Vulnerable To Pre-Authentication RCE

#### Description

Erlang/OTP is a set of libraries for the Erlang programming language. Prior to versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20, a SSH server may allow an attacker to perform unauthenticated remote code execution (RCE). By exploiting a flaw in SSH protocol message handling, a malicious actor could gain unauthorized access to affected systems and execute arbitrary commands without valid credentials. This issue is patched in versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20. A temporary workaround involves disabling the SSH server or to prevent access via firewall rules.

CWE 1 Total  
[Learn more](#)

- CWE-306: CWE-306: Missing Authentication for Critical Function

CVSS 1 Total  
[Learn more](#)

Score	Severity	Version	Vector String
10.0	CRITICAL	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

#### Product Status

[Learn more](#)

Vendor	Product
erlang	otp

Versions 3 Total

Default Status: unknown

#### On This Page

Required CVE Record Information

- CNA: GitHub (Maintainer Security Advisories)
- CVE Program

Authorized Data Publishers

- CISA-ADP

Эта уязвимость имеет следующие параметры:

Оценка: 10.0

Серьезность: Критическая

Вектор: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (версия 3.1)

Тип ошибки: Отсутствие аутентификации для критичной функции (CWE-306)

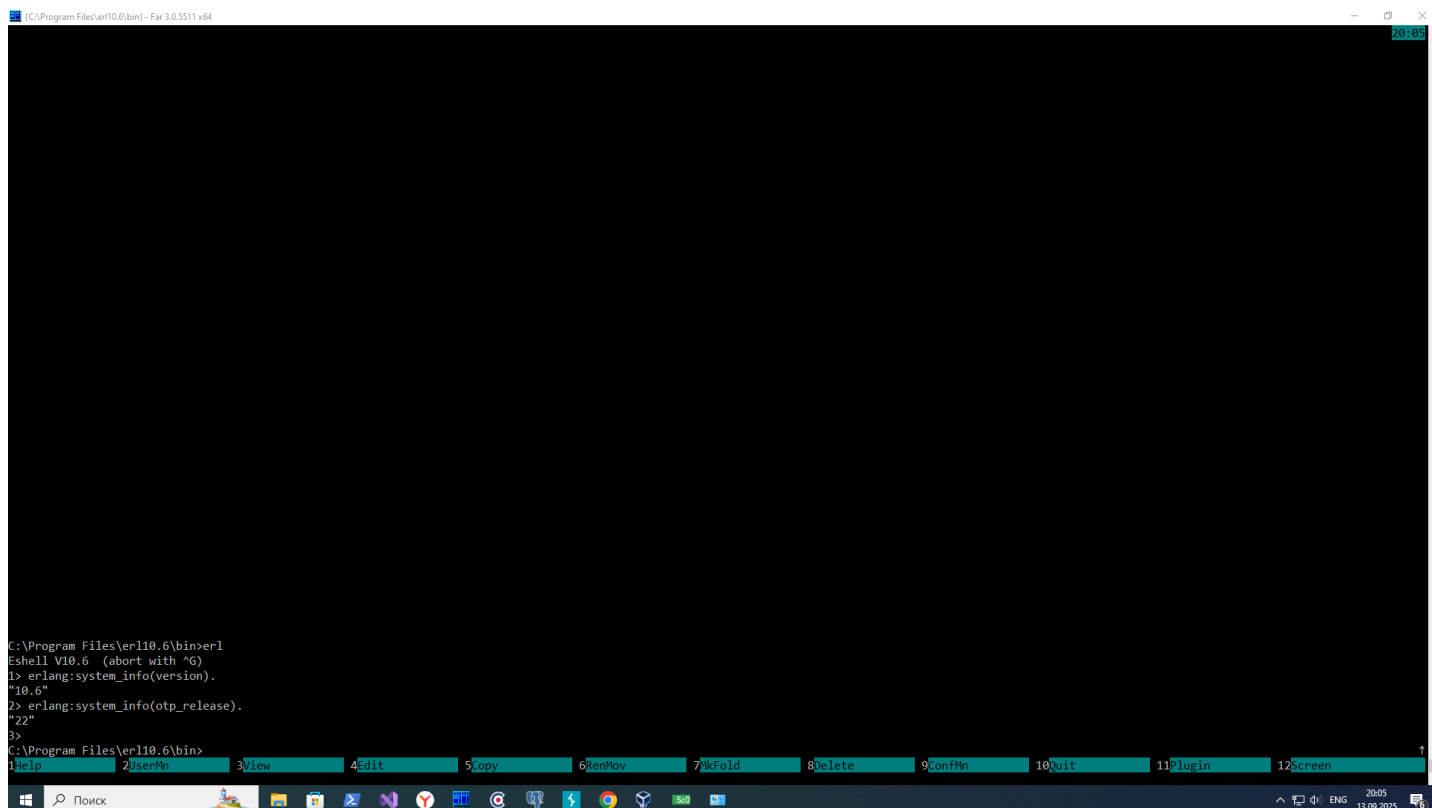
Описание уязвимости: Уязвимость реализации протокола SSH из набора библиотек Erlang/OTP связана с отсутствием проверки подлинности для критически важной функции. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированных SSH-пакетов.

Описание уязвимости на cve.org: Erlang/OTP is a set of libraries for the Erlang programming language. Prior to versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20, a SSH server may allow an attacker to perform unauthenticated remote code execution (RCE). By exploiting a flaw in SSH protocol message handling, a malicious actor could gain unauthorized access to affected systems and execute arbitrary commands without valid credentials. This issue is patched in versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20. A temporary workaround involves disabling the SSH server or to prevent access via firewall rules.

Возможные меры по устранению уязвимости: Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

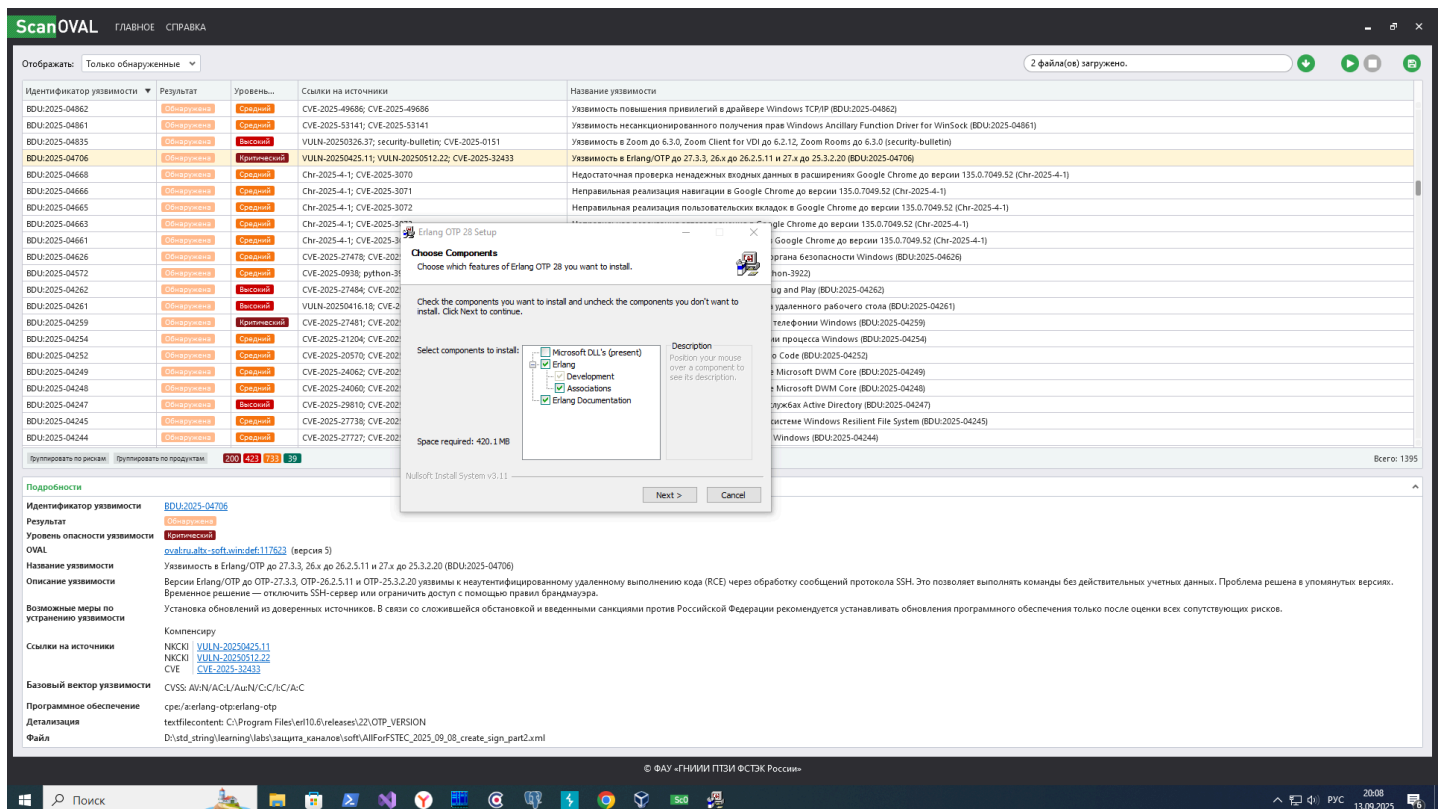
Устраняю уязвимость.

Проверяю текущую версию Erlang/OTP:

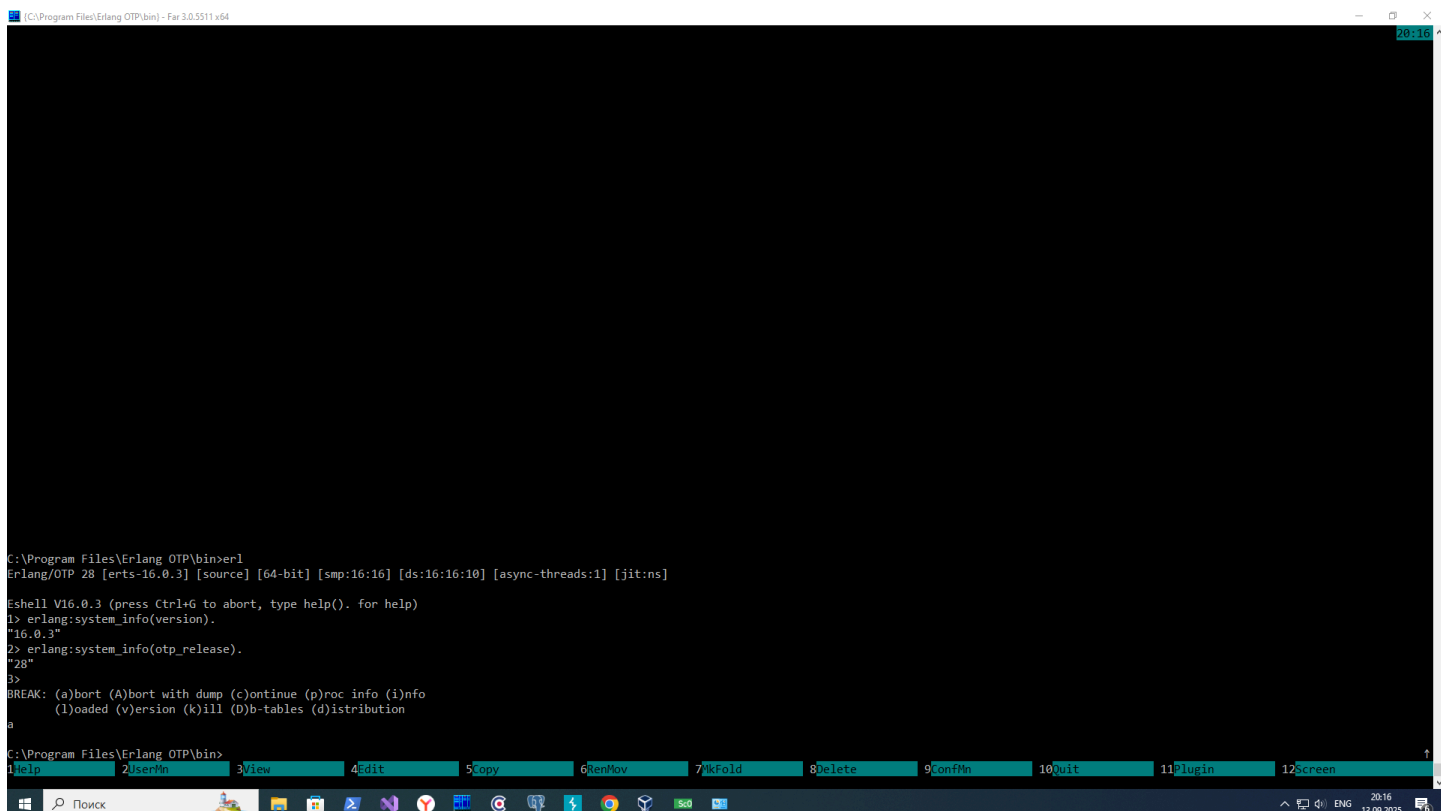
A screenshot of a Windows command prompt window titled "C:\Program Files\erl10.6\bin - Far 3.0.5511 x64". The window shows the execution of the Erlang shell (Eshell V10.6) and the output of two commands: `erlang:system_info(version).` which returns `"10.6"`, and `erlang:system_info(otp_release).` which returns `"22"`. The command prompt has a menu bar with options like Help, UserIn, View, Edit, Copy, RenMov, FileFold, Delete, ConfMn, Quit, Plugin, and Screen. The Windows taskbar at the bottom shows the date as 13.09.2023 and the time as 20:05.

```
C:\Program Files\erl10.6\bin>erl
Eshell V10.6 (abort with ^G)
1> erlang:system_info(version).
"10.6"
2> erlang:system_info(otp_release).
"22"
3>
C:\Program Files\erl10.6\bin>
```

Обновляю Erlang/OTP до последней версии:



Проверяю версию Erlang/OTP после обновления:



Запускаю сканирование хостовой машины с помощью ScanOVAL после устранения уязвимости:



