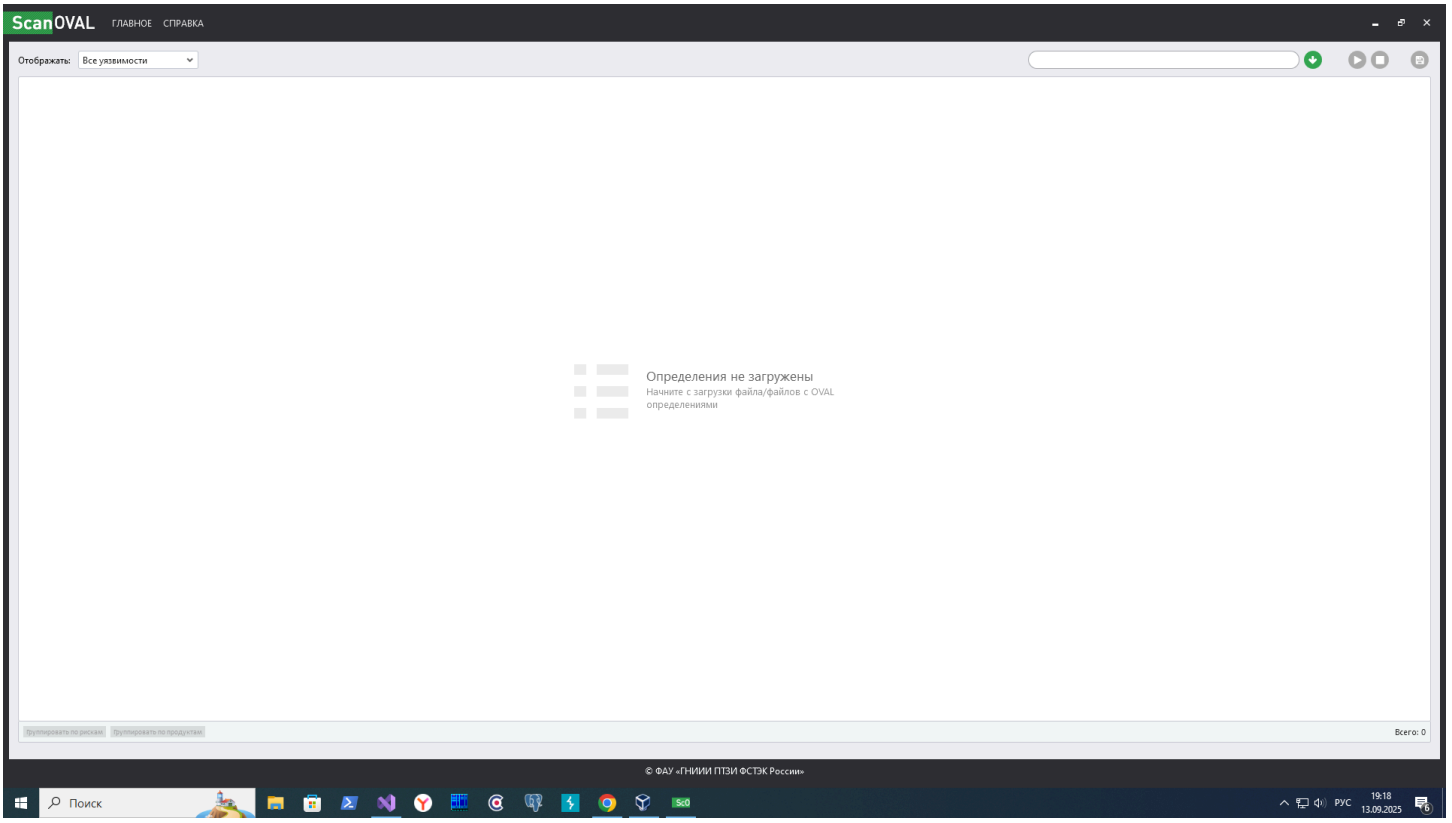
Задание:

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:

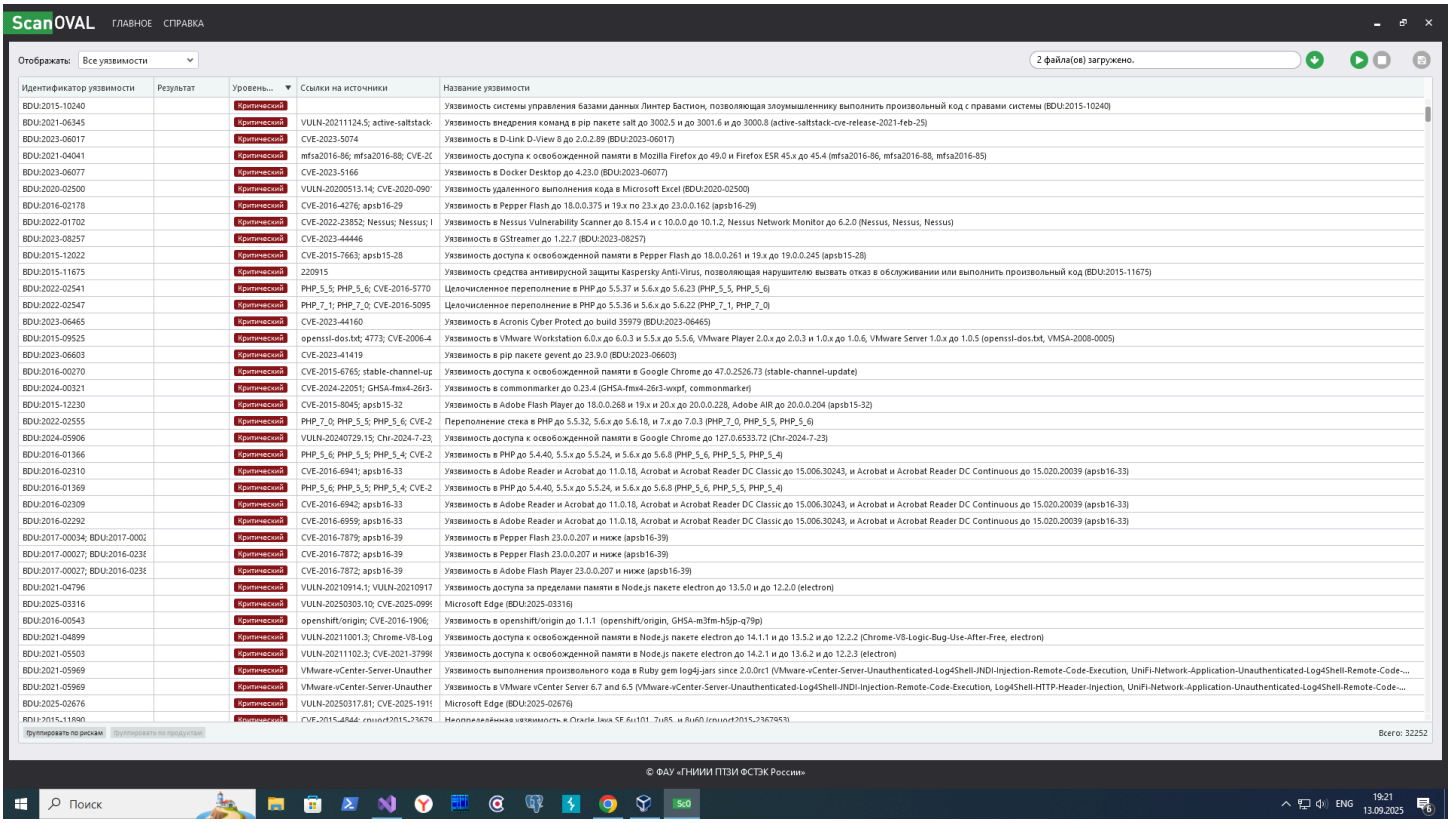
- Что уязвимо?
- Как может быть реализована уязвимость?
- Прочитать описание на CVE?
- Как устранить уязвимость?

3. Устраните уязвимости.
4. Проведите повторное сканирование.

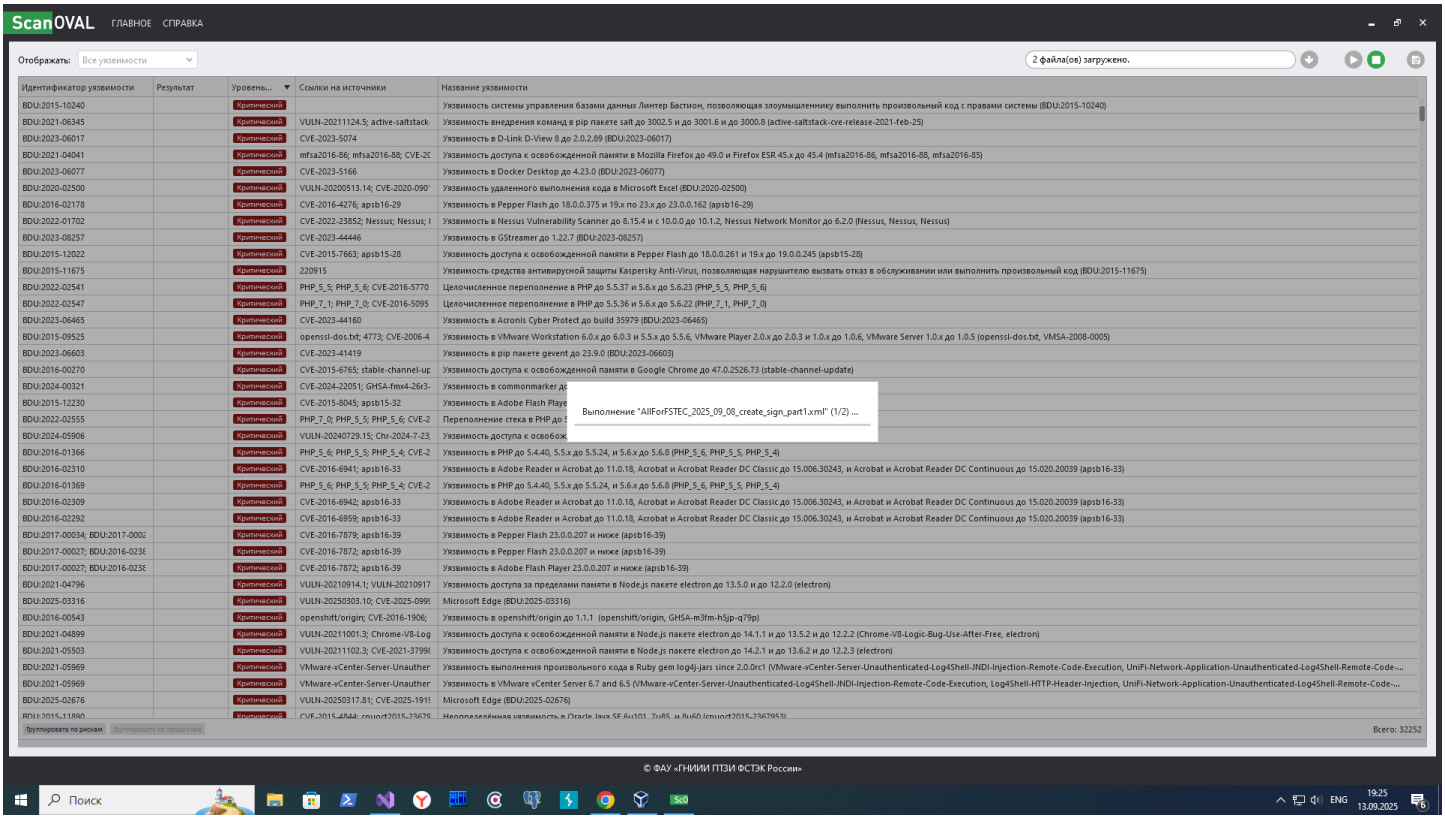
Я буду использовать сканер ScanOVAL.
Запускаю сканер ScanOVAL:

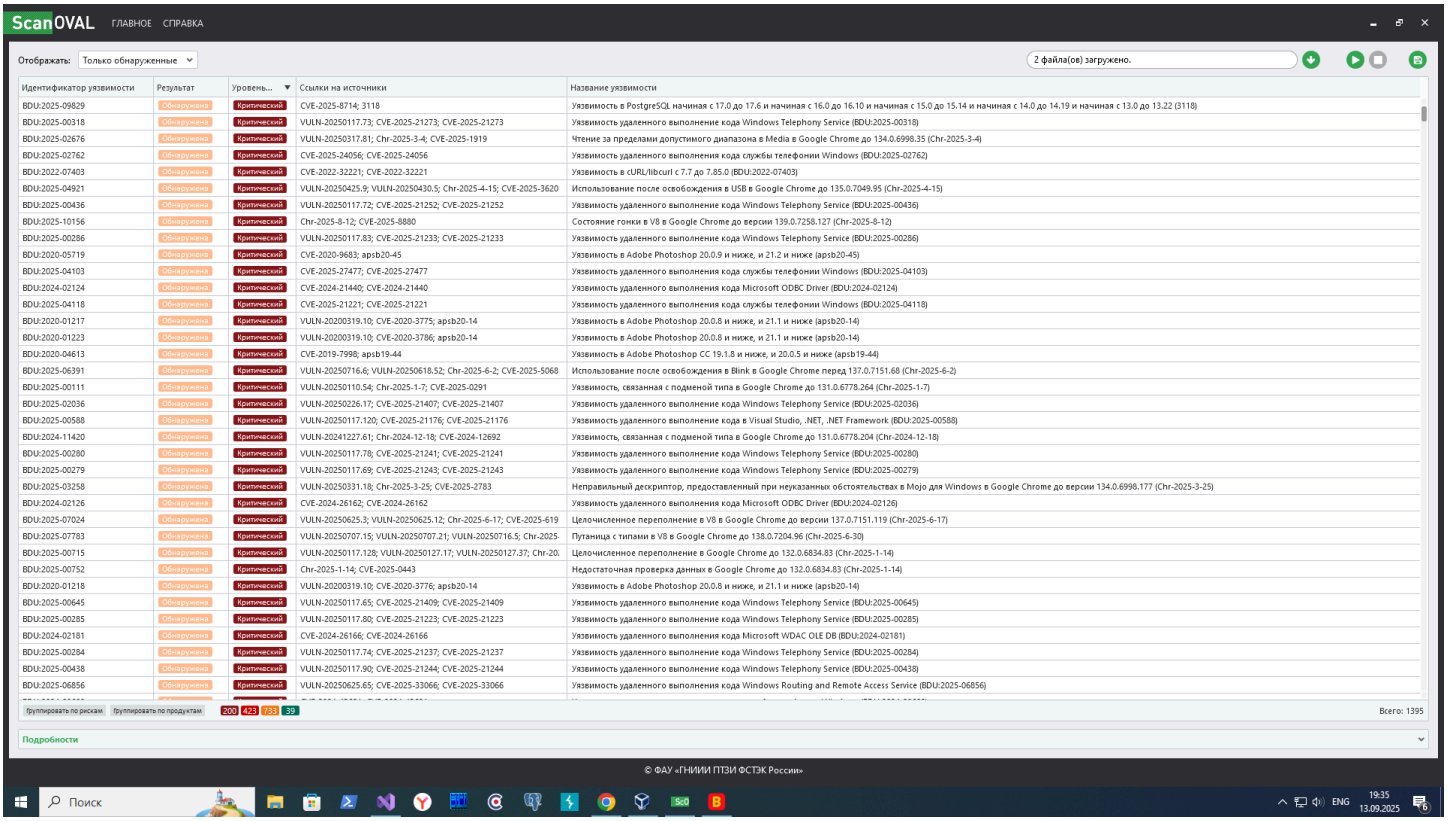


Загружаю базу OVAL определений

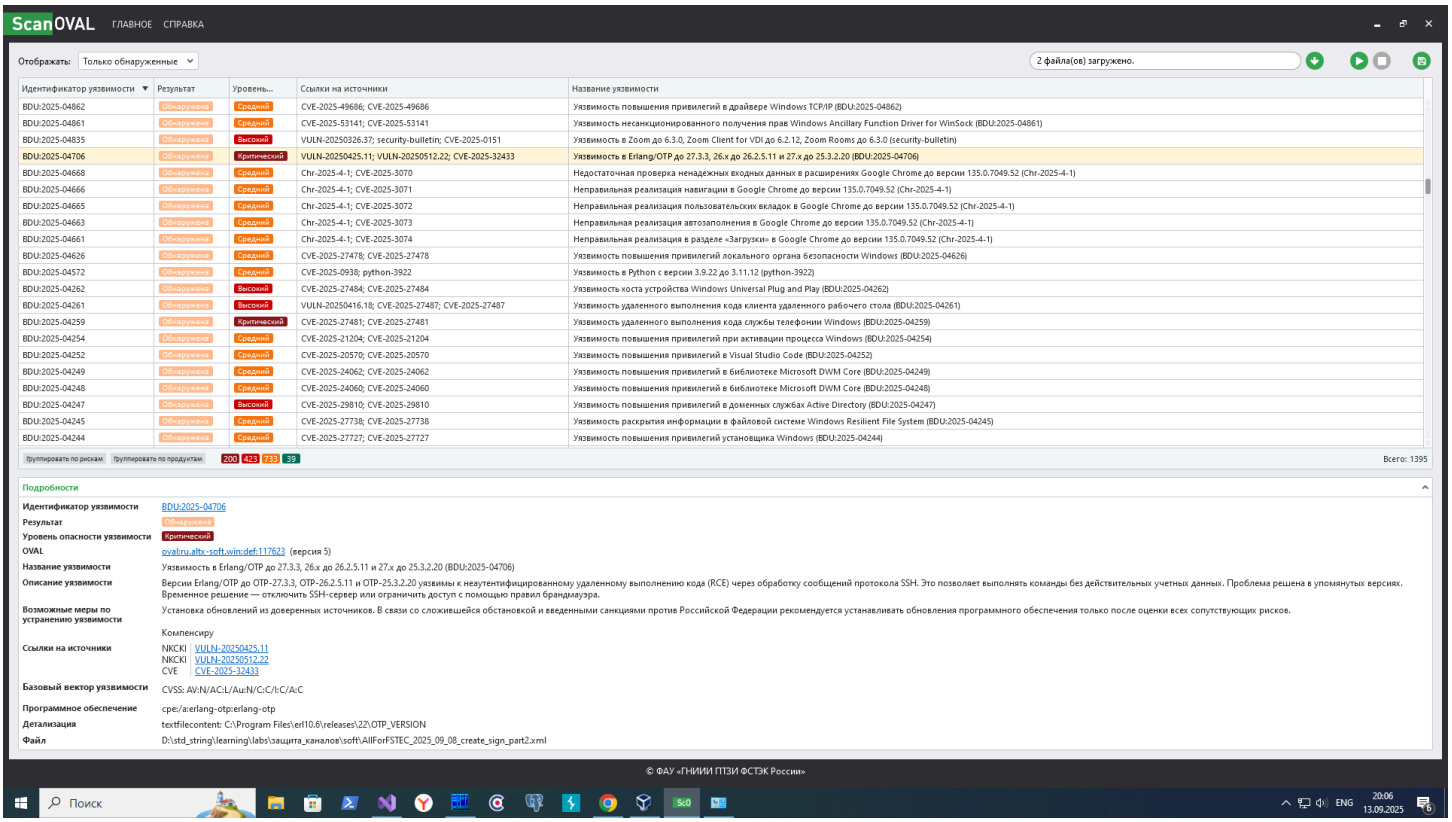


Запускаю сканирование хостовой машины с помощью ScanOVAL

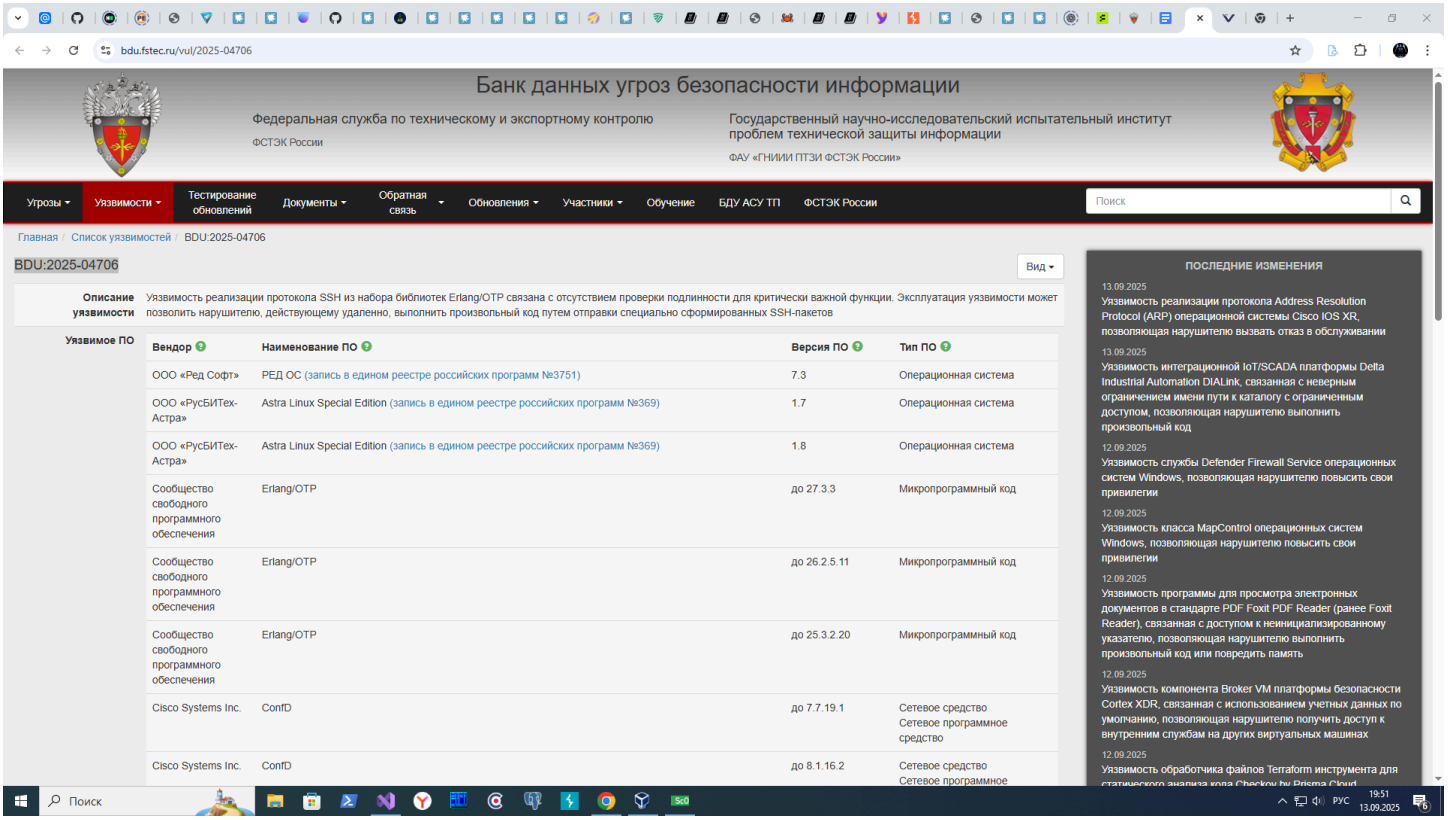




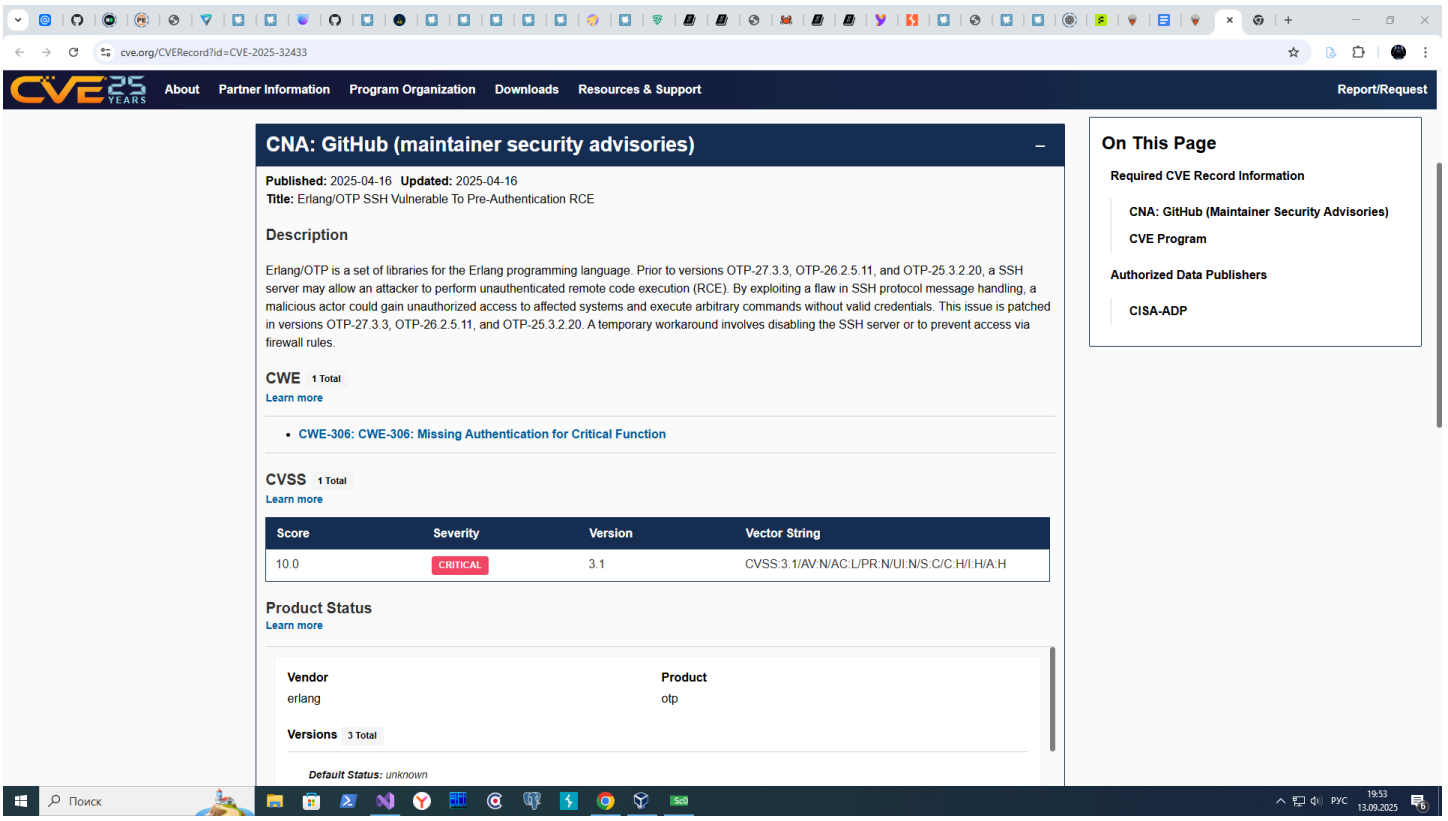
Выбираю одну критическую уязвимость. В качестве такой уязвимости я беру уязвимость BDU:2025-04706 (CVE-2025-32433)



Вот описание этой уязвимости на сайте ФСТЭК:



Вот описание этой уязвимости на cve.org:



Эта уязвимость имеет следующие параметры:

Оценка: 10.0
Серьезность: Критическая

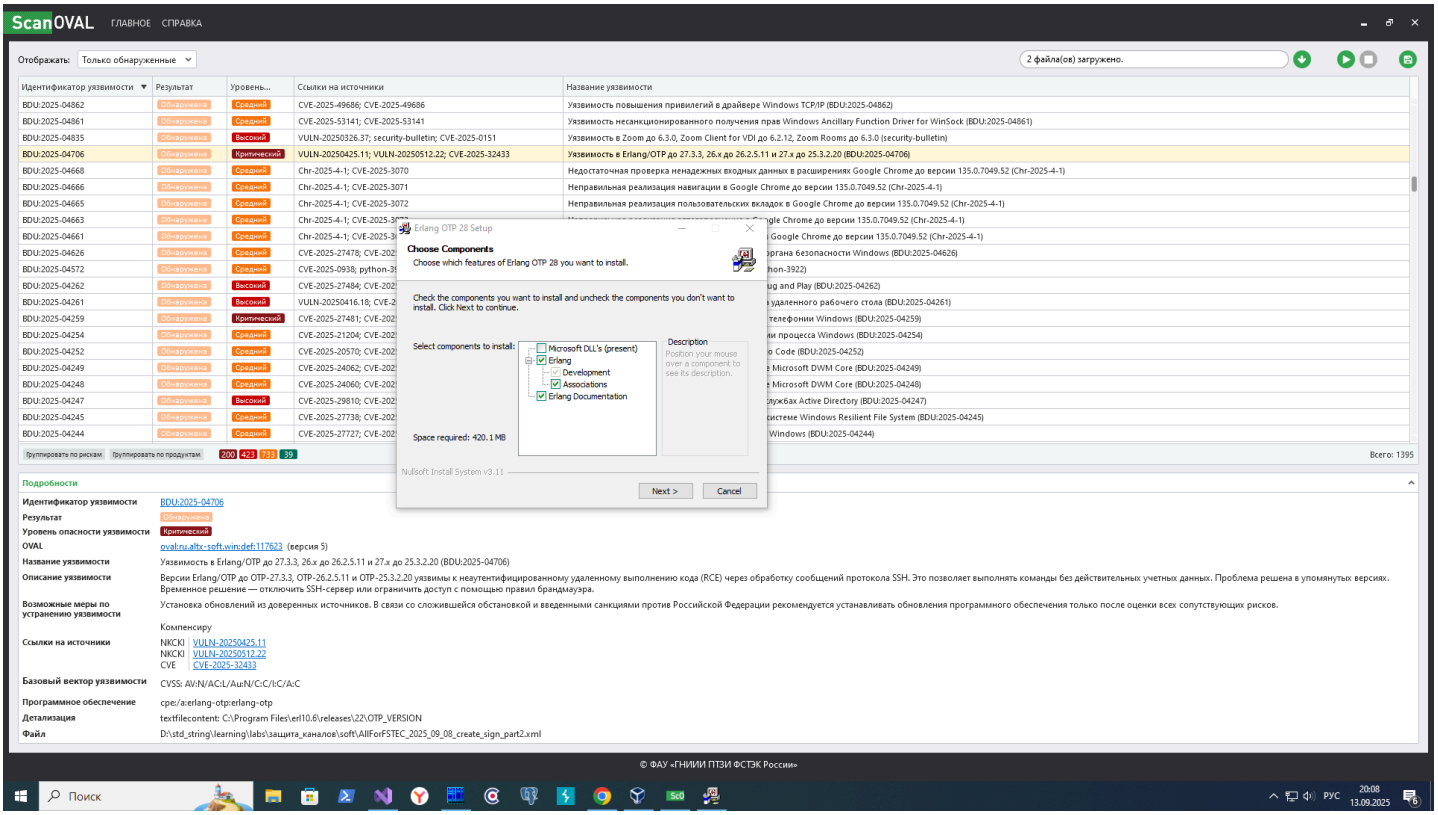
Вектор: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (версия 3.1)
Тип ошибки: Отсутствие аутентификации для критичной функции (CWE-306)

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.

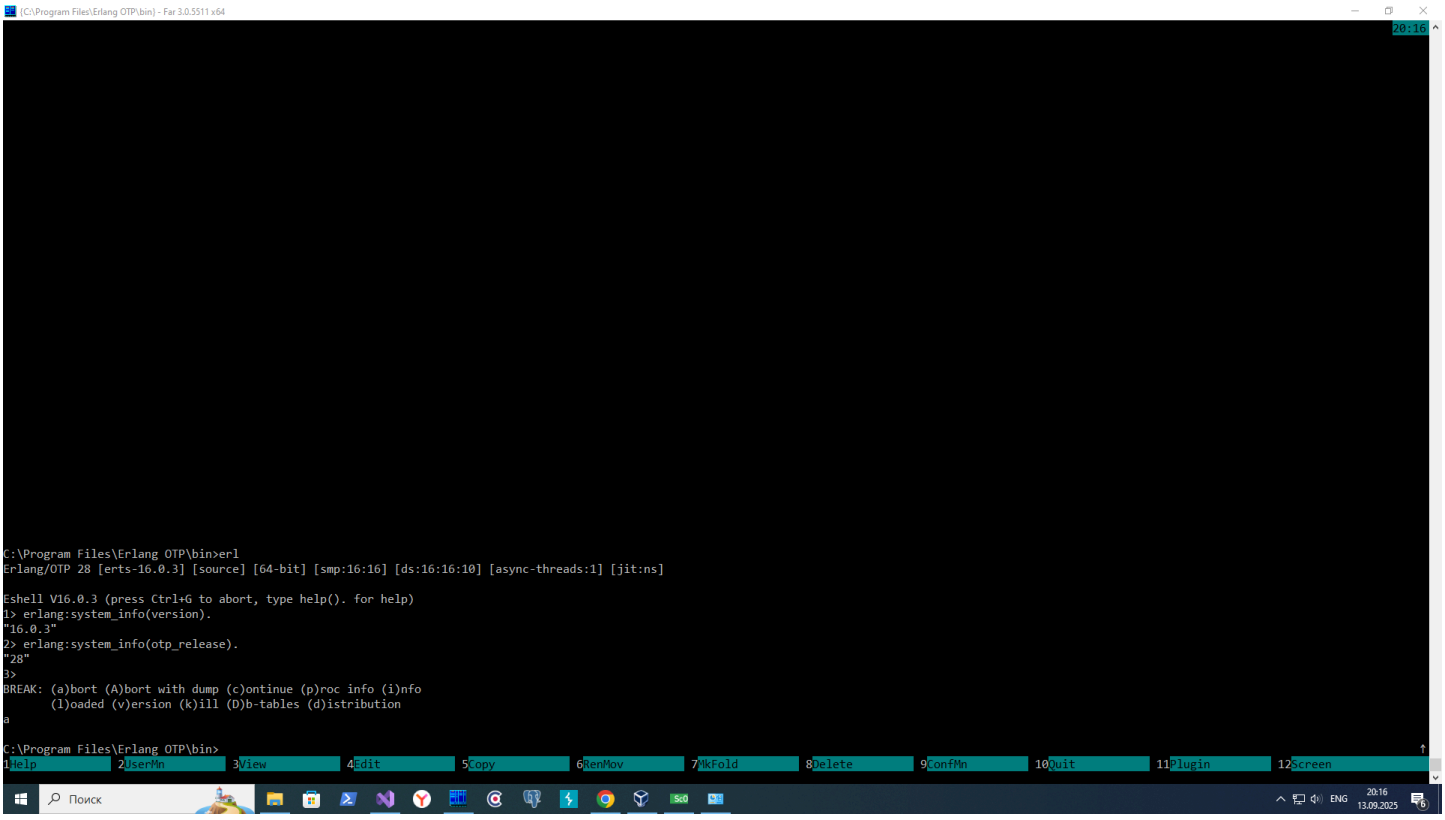
Описание уязвимости на cve.org: Erlang/OTP is a set of libraries for the Erlang programming language. Prior to versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20, a SSH server may allow an attacker to perform unauthenticated remote code execution (RCE). By exploiting a flaw in SSH protocol message 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:

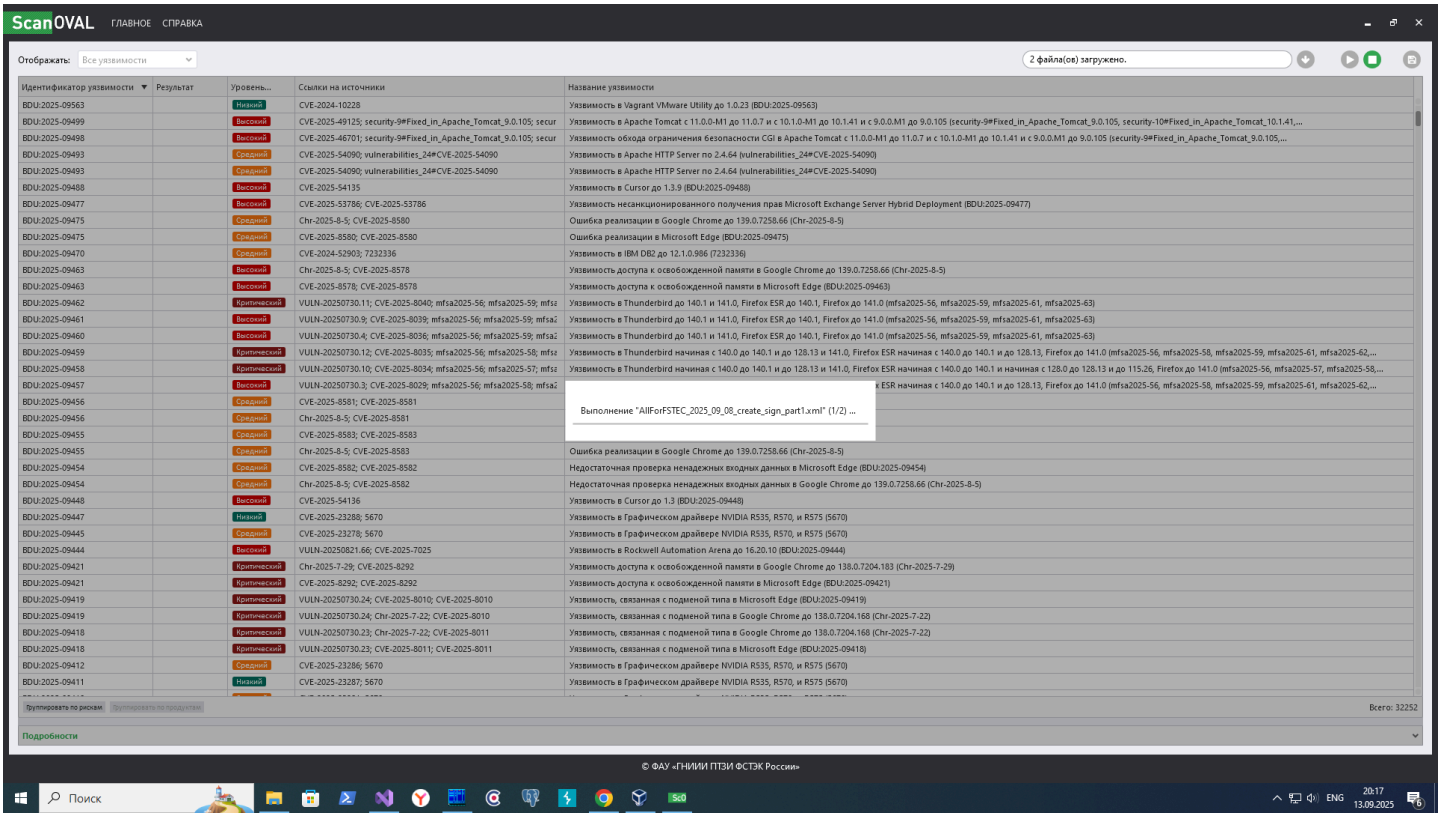
Обновляю Erlang/OTP до последней версии:



Проверяю версию Erlang/OTP после обновления:



Запускаю сканирование хостовой машины с помощью ScanOVAL после устранения уязвимости:



Видно, что уязвимости BDU:2025-04706 (CVE-2025-32433) среди найденных уязвимостей больше нет