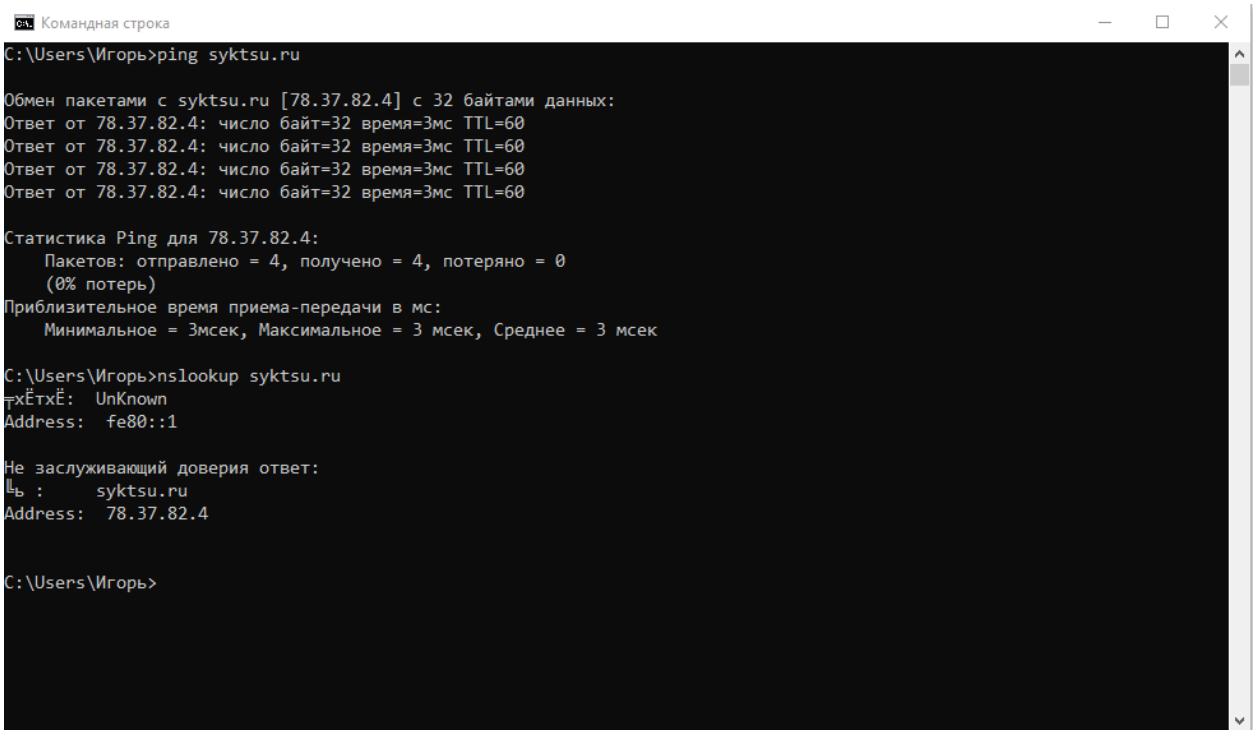
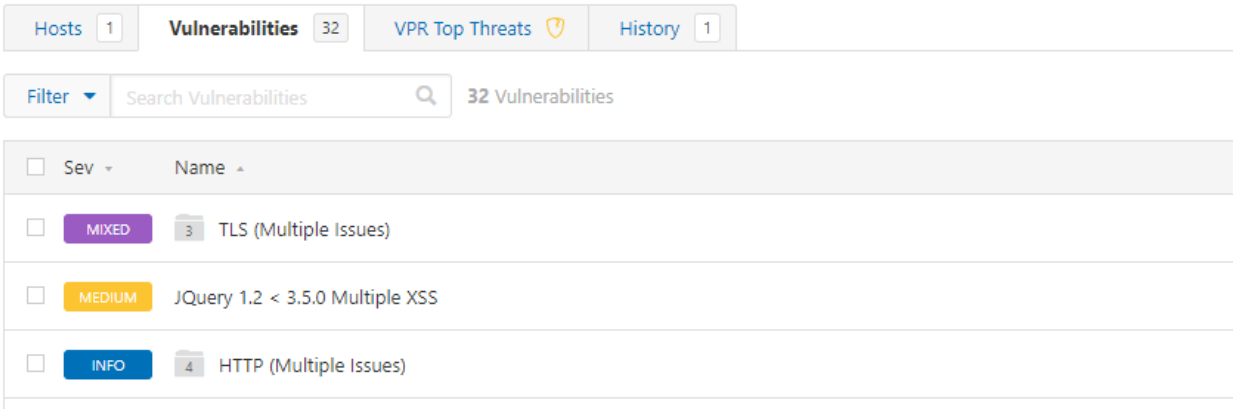
Анализ уязвимостей веб-сайта syktsu.ru с помощью сканера Nessus

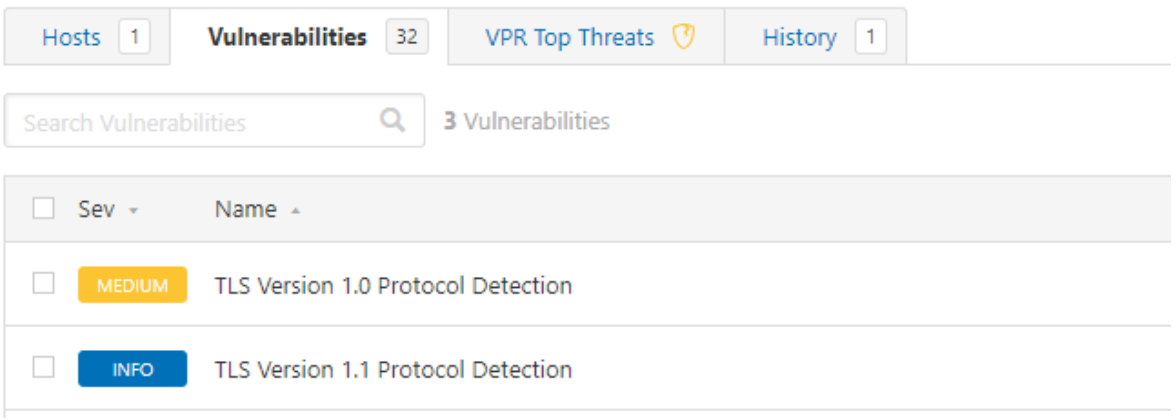
Узнаем ip адрес сайта: 78.37.82.4



Производим сканирование и видим, что было найдено две medium уязвимости:

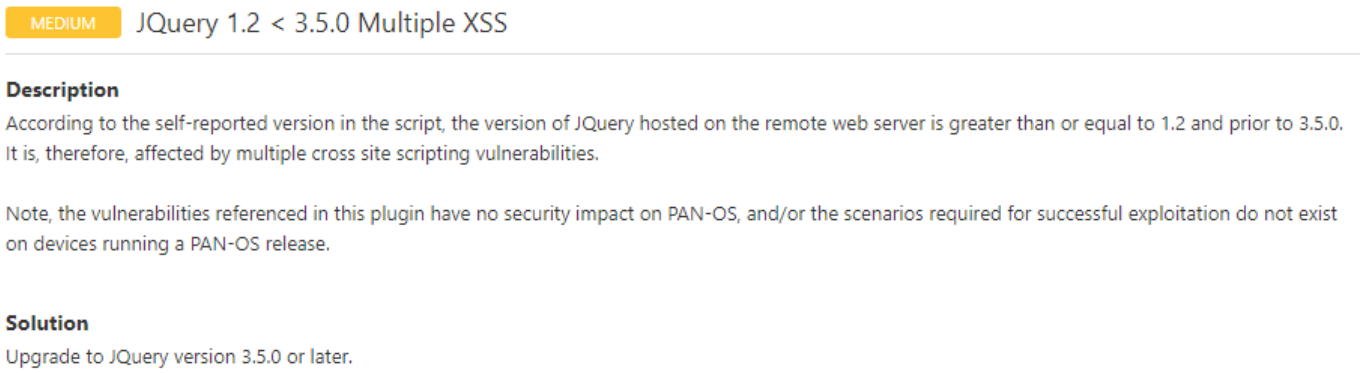


Одна из них в разделе TSL:



Первая уязвимость «*JQuery 1.2 < 3.5.0 Multiple XSS*» говорит о старой версии JQuery, установленной на сервере, что в свою очередь позволяет использовать многочисленные уязвимости, имеющиеся в этой версии.

Решение: обновить до версии 3.5.0 или более поздней.



MEDIUM JQuery 1.2 < 3.5.0 Multiple XSS

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

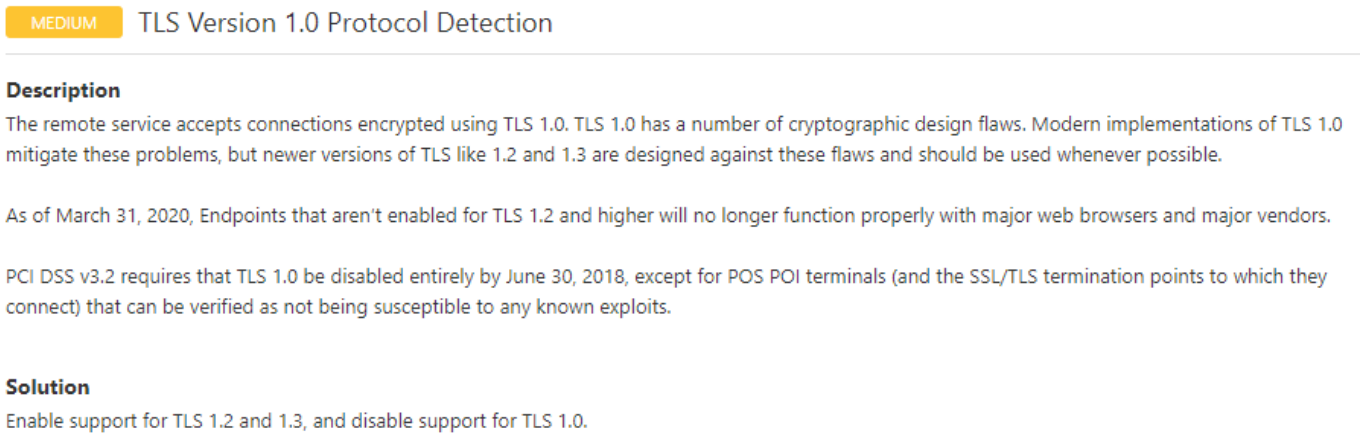
Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

Solution

Upgrade to JQuery version 3.5.0 or later.

Вторая уязвимость «*TLS Version 1.0 Protocol Detection*». Сайт принимает соединения, зашифрованные с помощью протокола TLS 1.0. Протокол TLS 1.0 подвержен использованию эксплойтов.

Решение: отключить поддержку TLS 1.0 и включить для TLS 1.2 и 1.3.



MEDIUM TLS Version 1.0 Protocol Detection

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Вывод: текущий уровень безопасности сайта вполне удовлетворительный. Были обнаружены две medium уязвимости, устранимые обновлением ПО.