

LDAP TLS漏洞测试

帅鹏

Version 1.0.0, April 5, 2023

# 文档编写目的

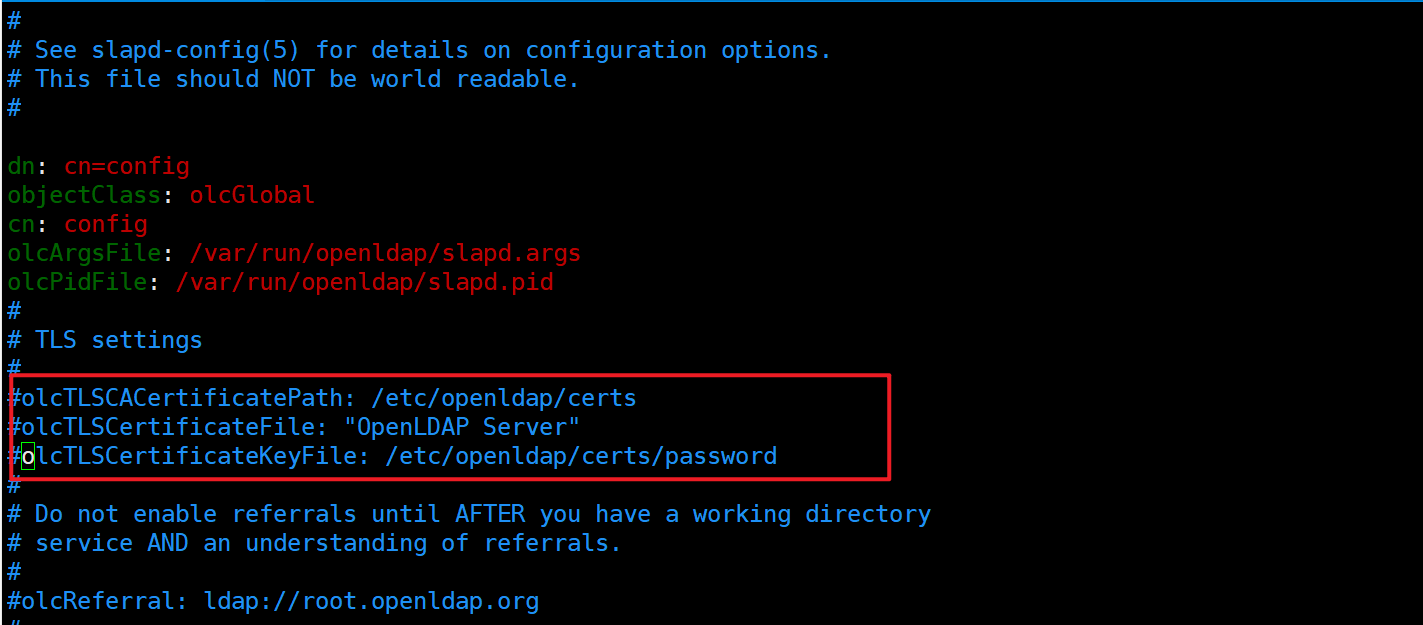
本文主要介绍在已部署的OpenLDAP基础上如何测试TLS1.0、TLS1.1的漏洞。

* 测试环境

1. OS版本为：Red Hat Enterprise 7.6
2. OpenLDAP版本为： 2.4.44
3. 操作用户：root

# 禁用LDAP的TLS测试TLS漏洞

修改slapd.ldif文件内容，注释掉TLS相关的配置

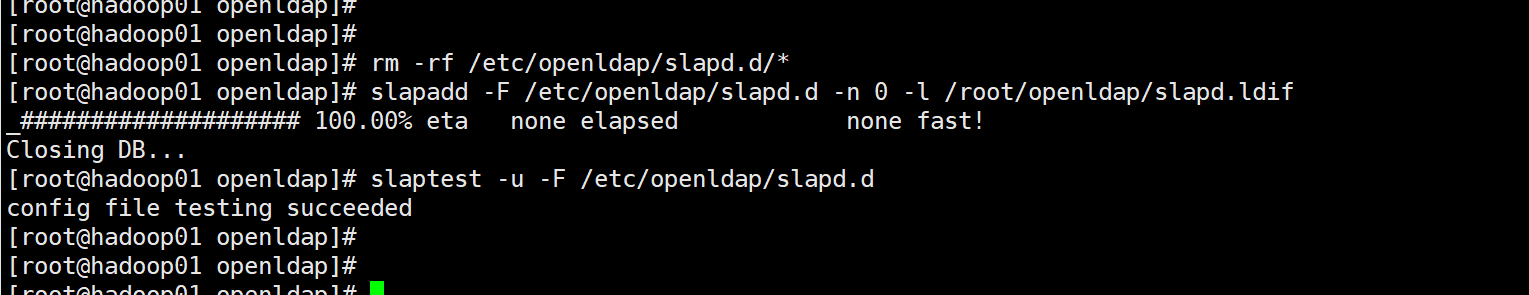


删除已有的配置，重新导入配置

rm -rf /etc/openldap/slapd.d/\*

slapadd -F /etc/openldap/slapd.d -n 0 -l /root/openldap/slapd.ldif

slaptest -u -F /etc/openldap/slapd.d



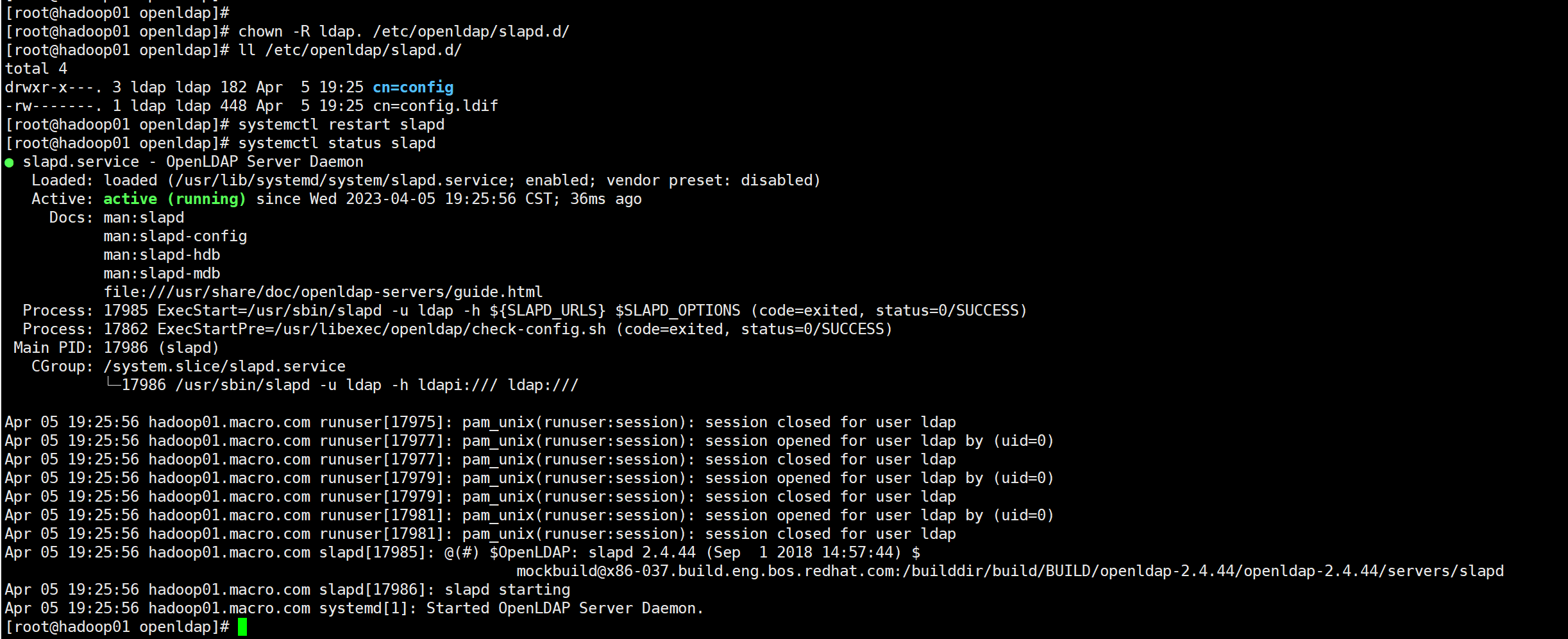
修改配置文件的属主，然后重启slapd服务

chown -R ldap. /etc/openldap/slapd.d/

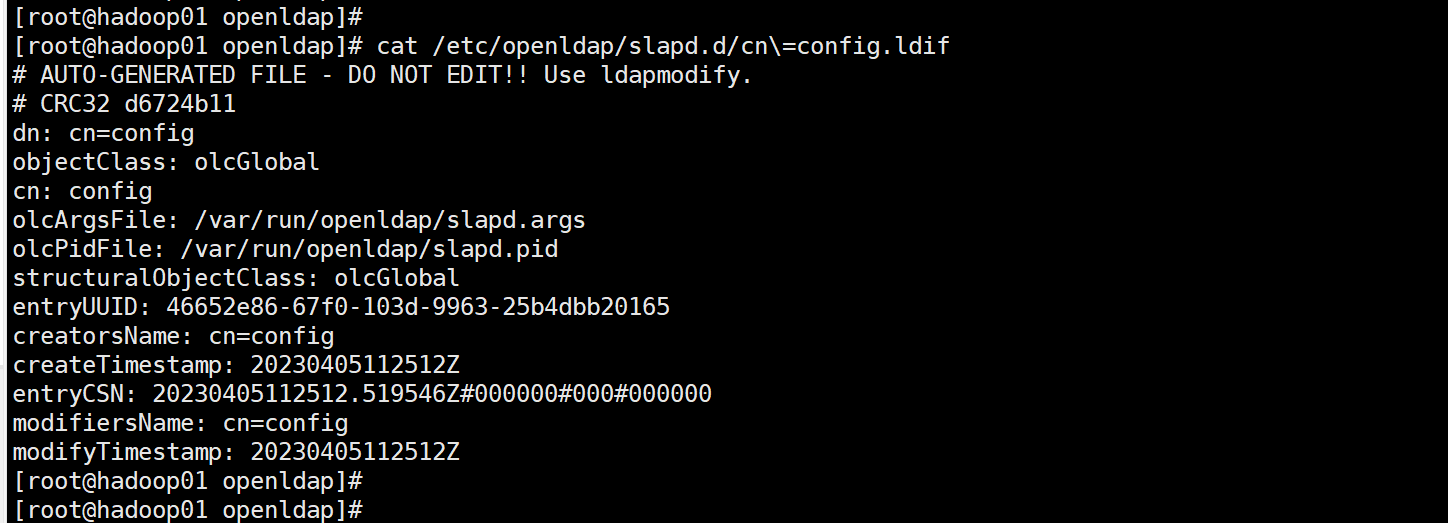
ll /etc/openldap/slapd.d/

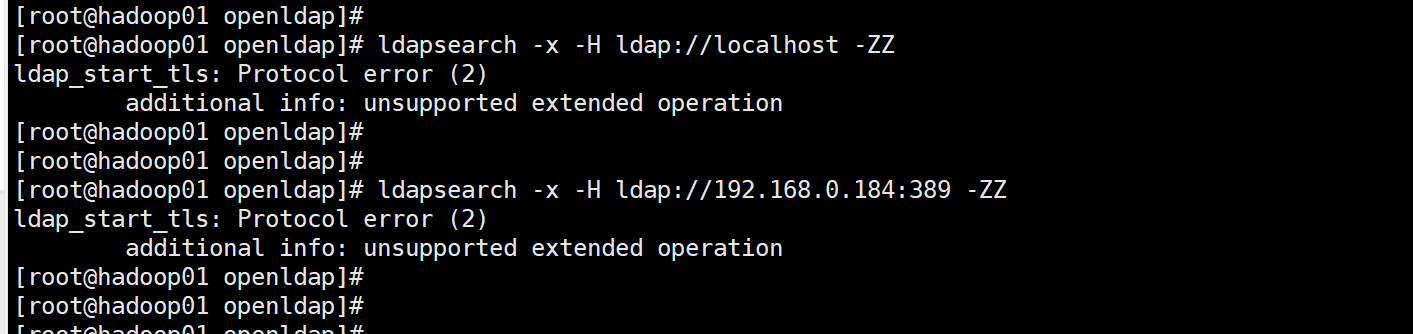
systemctl restart slapd

systemctl status slapd

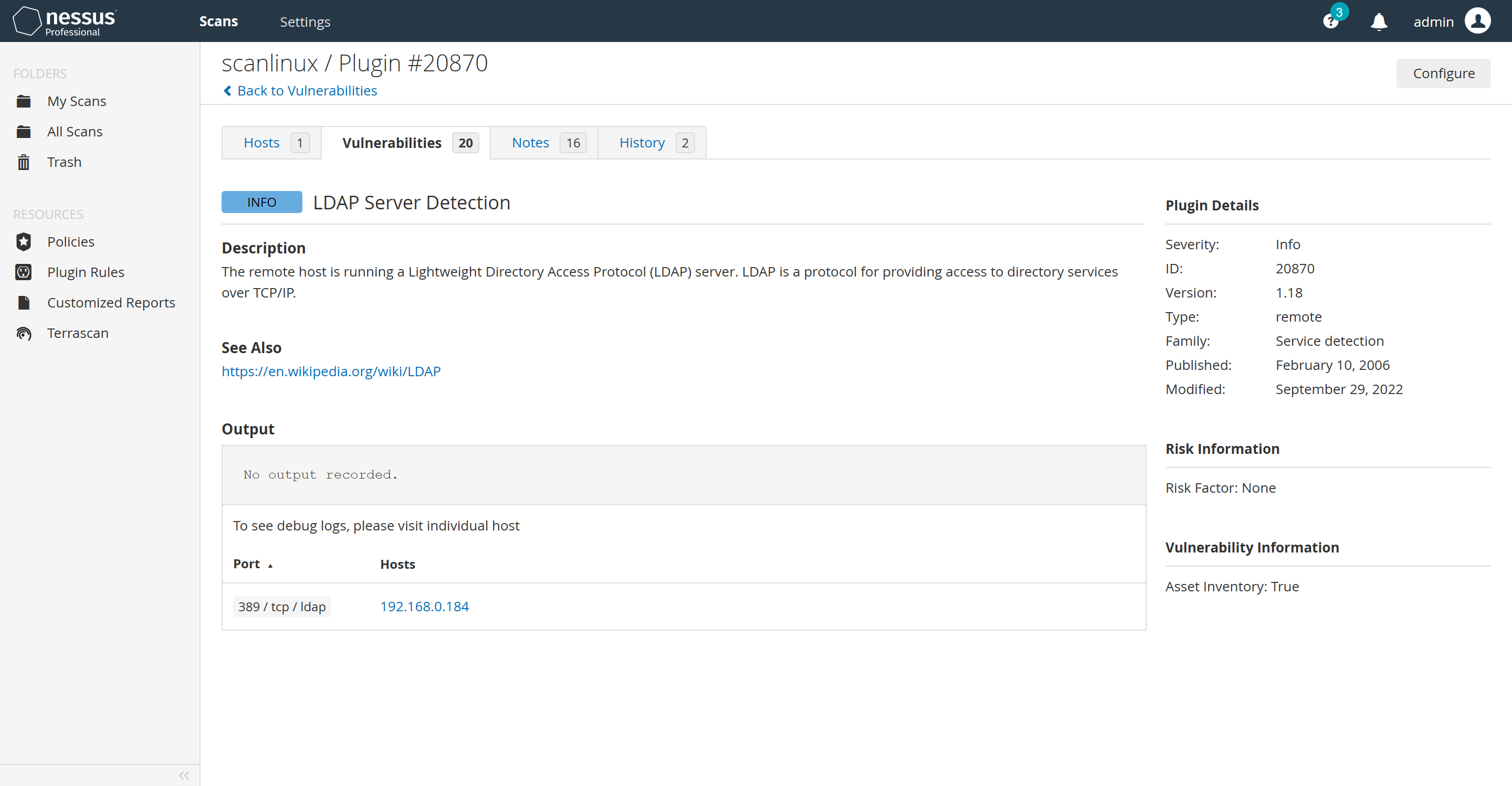
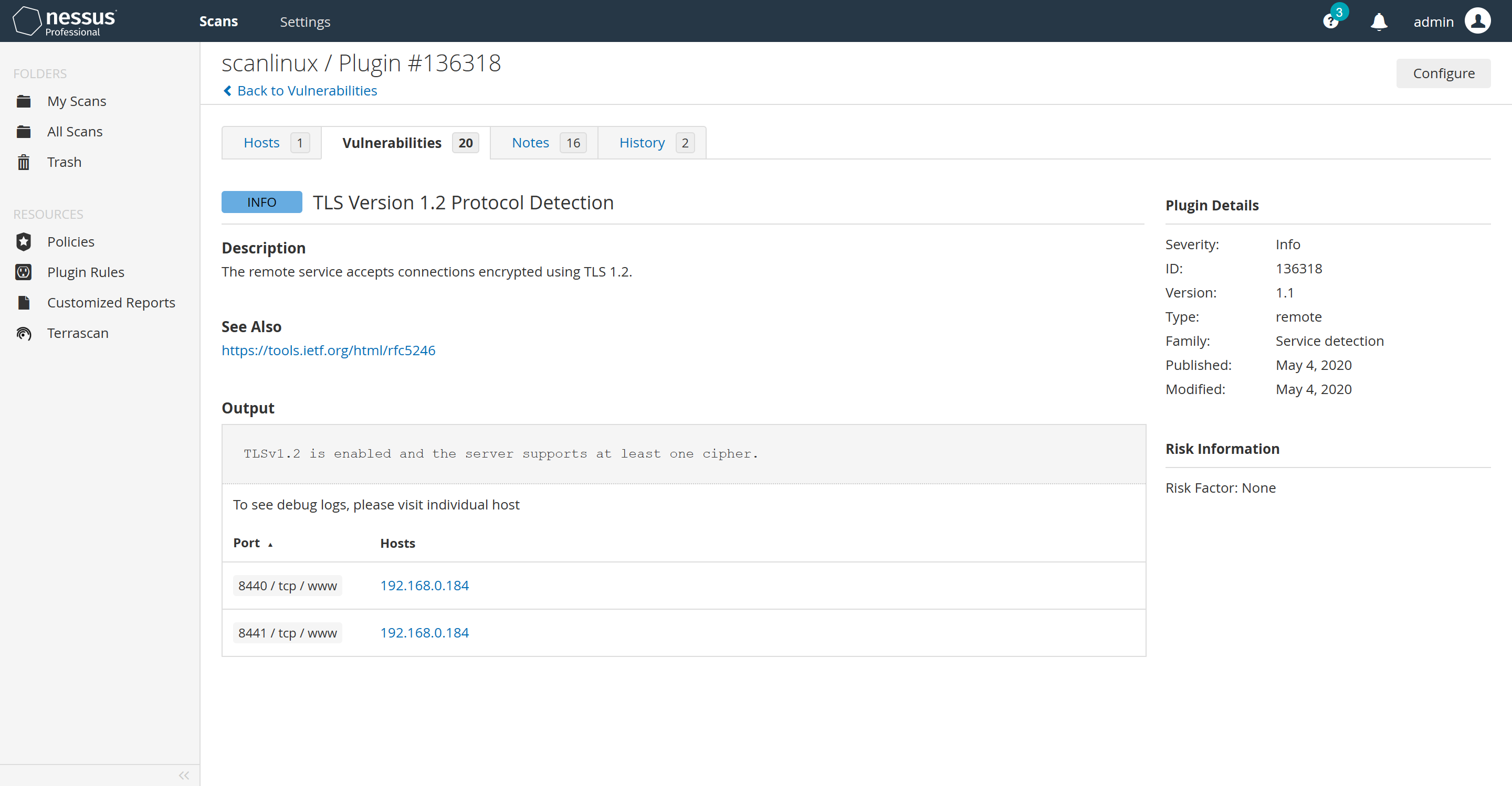
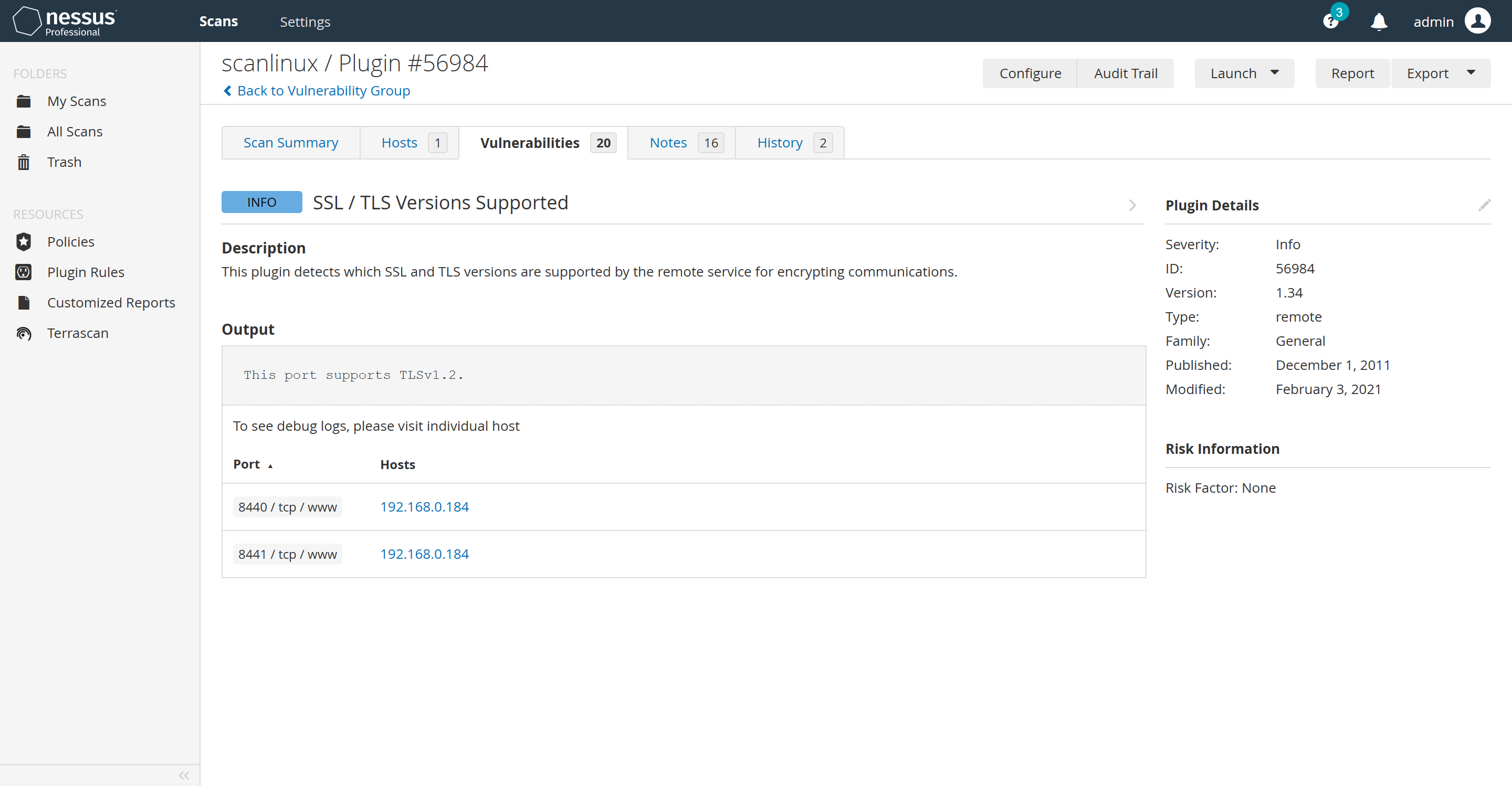
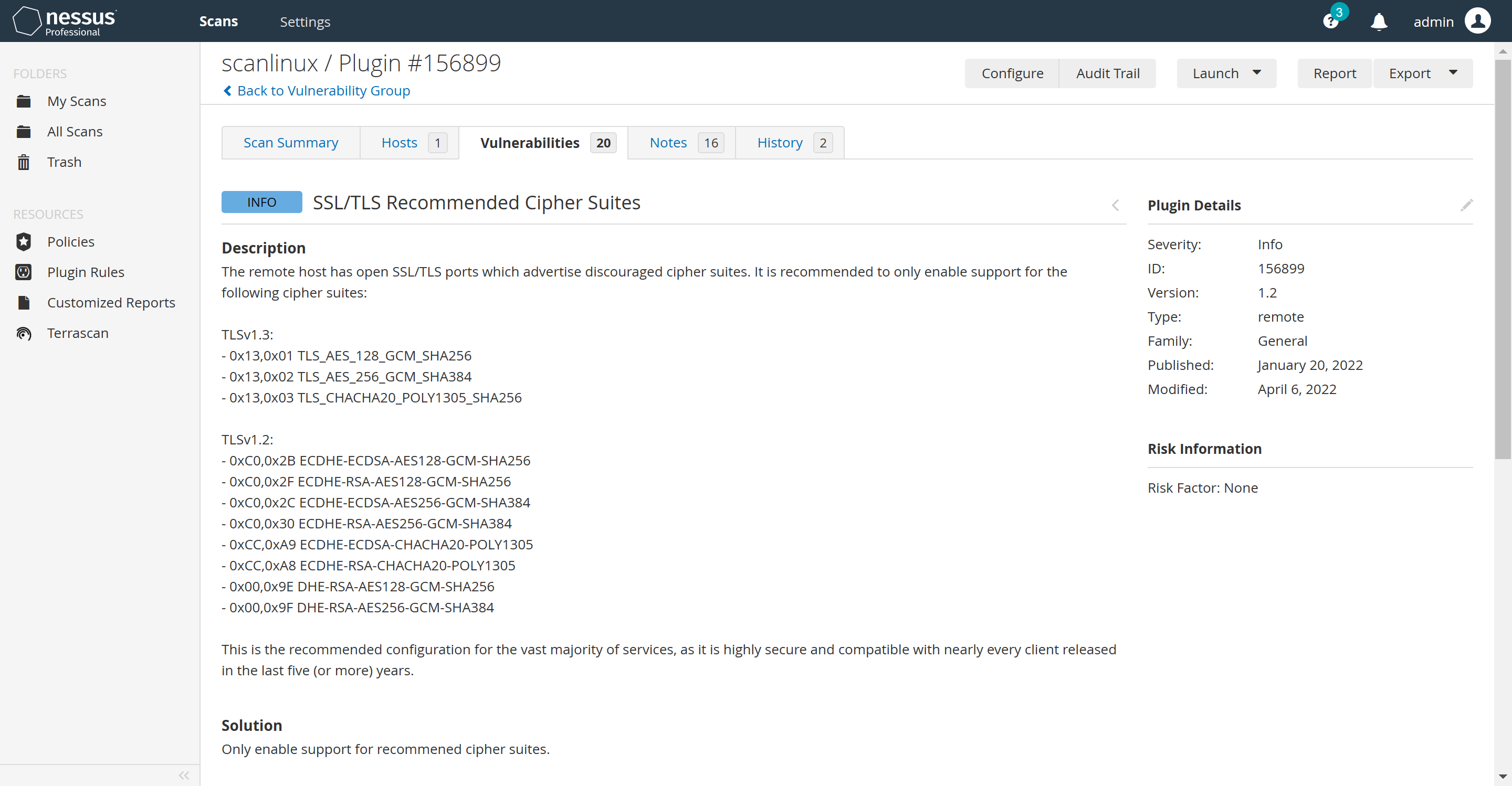
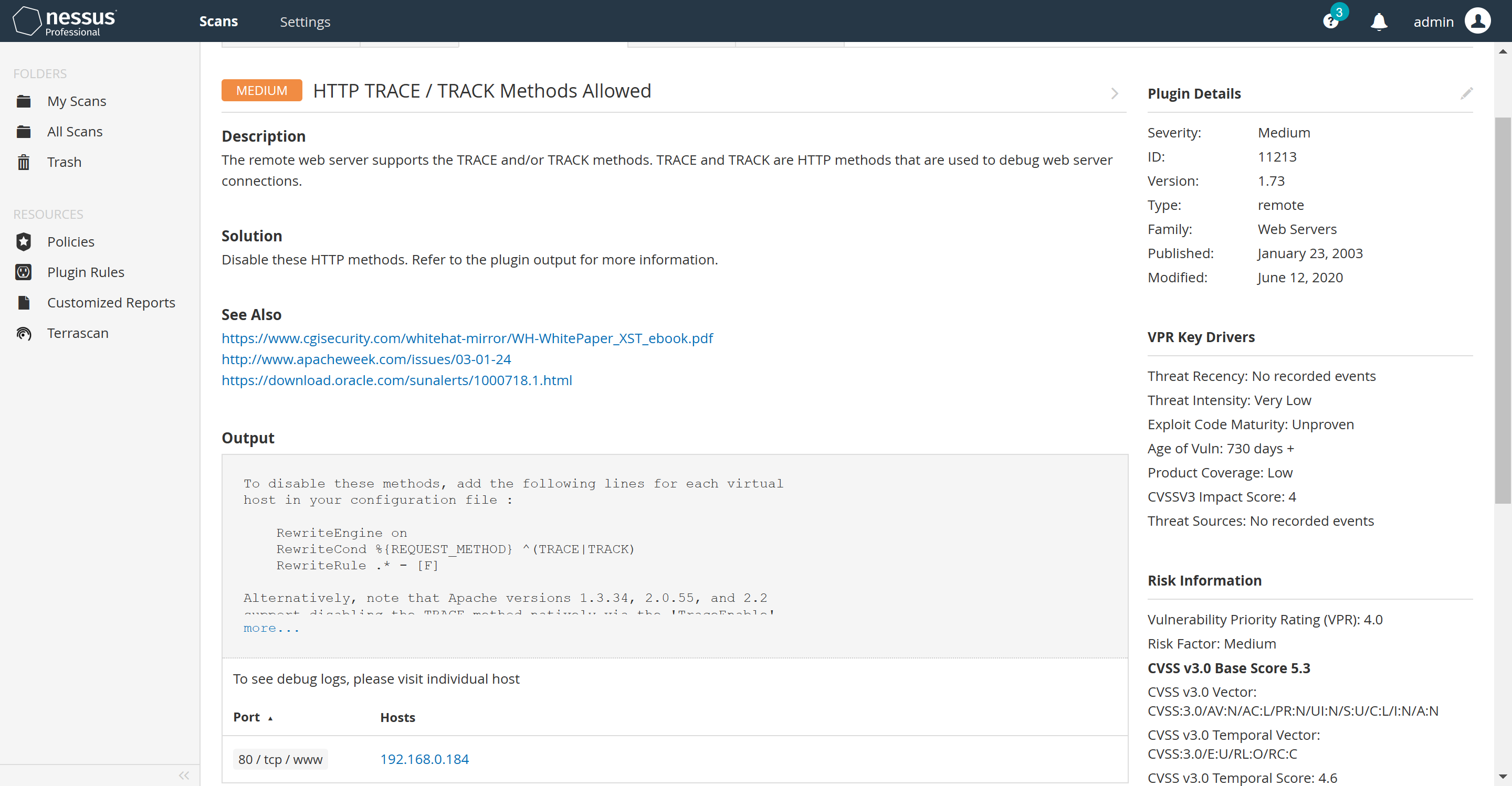


确认LDAP已经禁用了TLS





使用Nessus漏洞扫描工具扫描主机

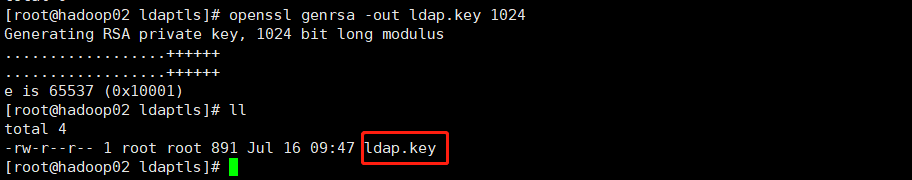
当前LDAP没有启用TLS的情况下，没有扫描出389端口的TLS漏洞，当前操作系统中的openssl的TLS版本为1.2，不支持TLSv1.0和TLSv1.1，因此也没有扫描出TLSv1.0和TLSv1.1的漏洞。

HTTP的80端口漏洞扫描出了，关闭HTTP服务即可。

# 启用LDAP的TLS测试TLS漏洞

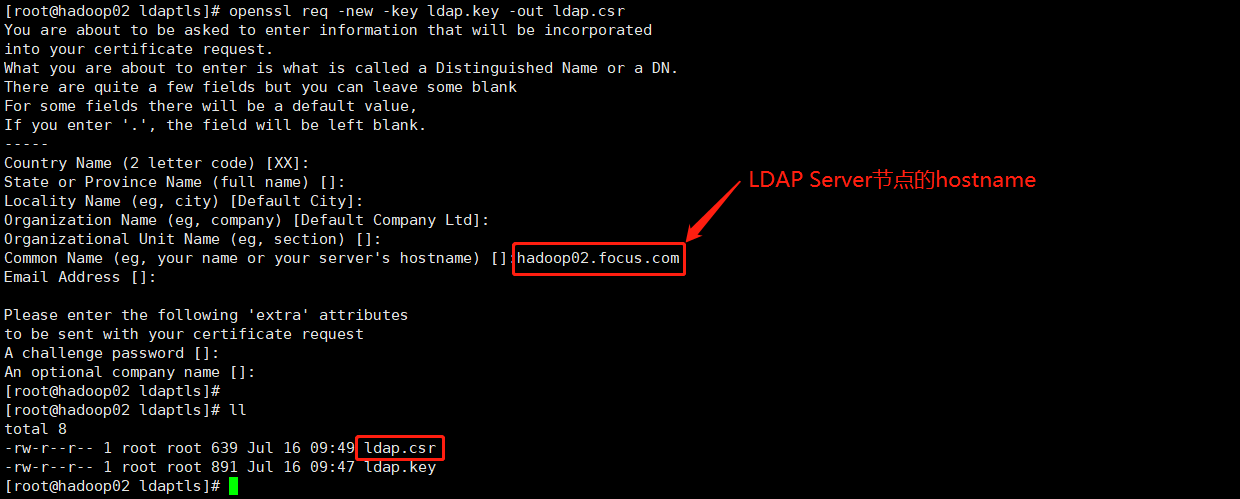
1. 生成RSA服务器私钥:

openssl genrsa -out ldap.key 1024



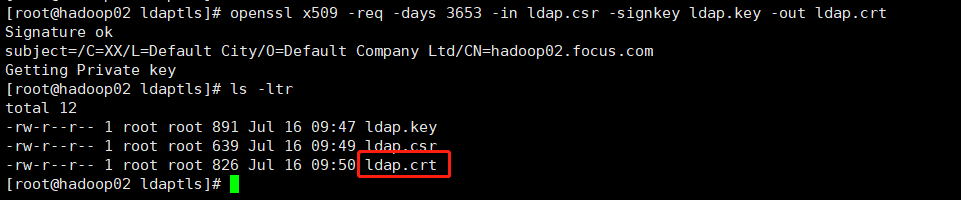
1. 生成签名文件:

openssl req -new -key ldap.key -out ldap.csr



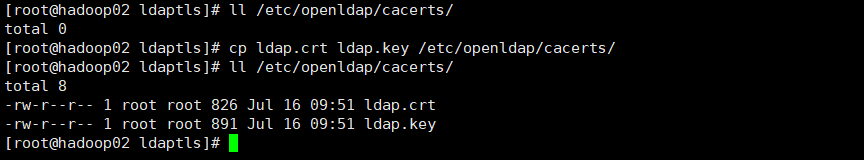
1. 生成公钥文件:

openssl x509 -req -days 3653 -in ldap.csr -signkey ldap.key -out ldap.crt



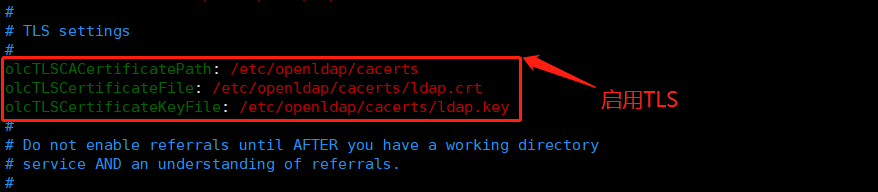
1. 将生成的公钥和私钥拷贝到/etc/openldap/cacerts/目录下:

cp ldap.crt ldap.key /etc/openldap/cacerts/



1. 修改slapd.ldif文件（默认位置：/usr/share/openldap-servers），添加TLS配置

vim /usr/share/openldap-servers/slapd.ldif

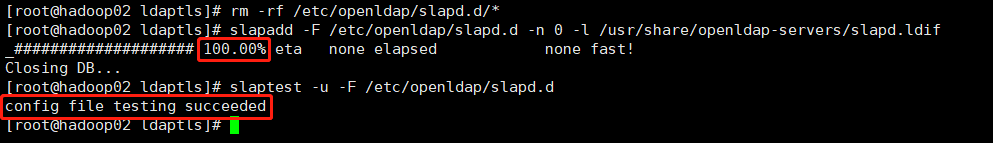


1. 如下命令重新生成OpenLDAP配置文件，并测试配置文件是否正确：

rm -rf /etc/openldap/slapd.d/\*

slapadd -F /etc/openldap/slapd.d -n 0 -l /root/openldap/slapd.ldif

slaptest -u -F /etc/openldap/slapd.d



执行如下命令修改配置文件的属主，然后重启slapd服务

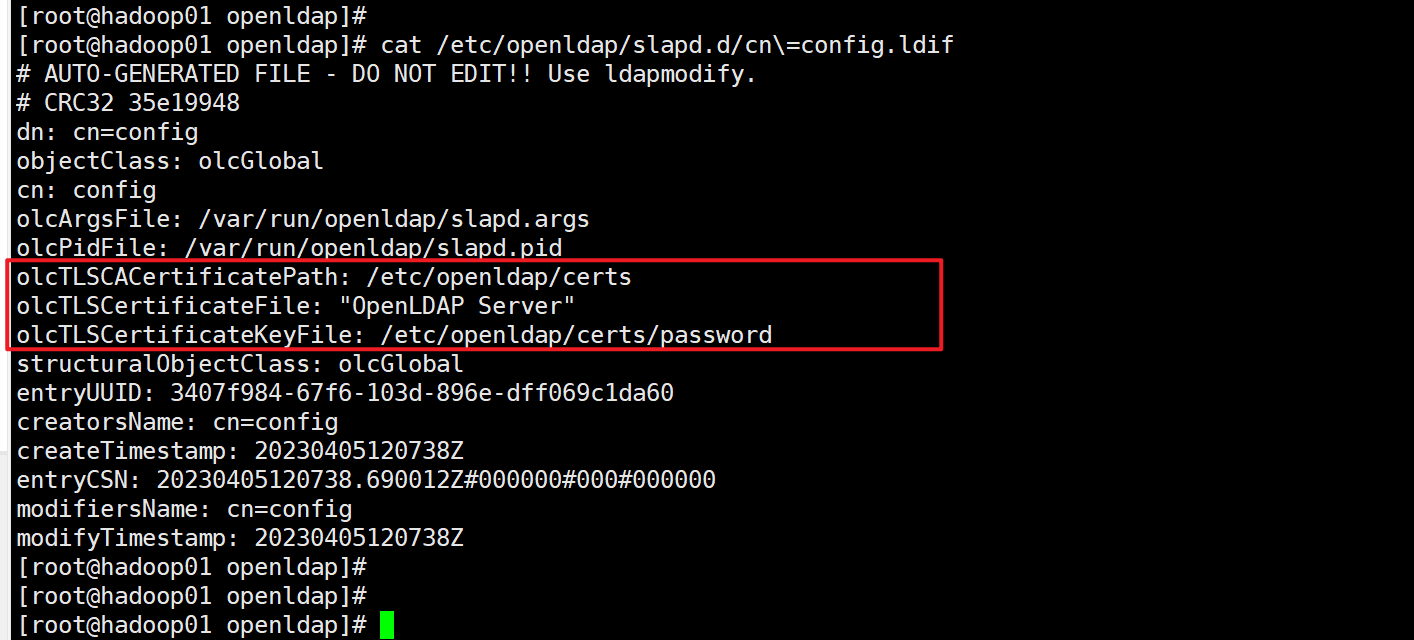
chown -R ldap. /etc/openldap/slapd.d/

ll /etc/openldap/slapd.d/

systemctl restart slapd

systemctl status slapd

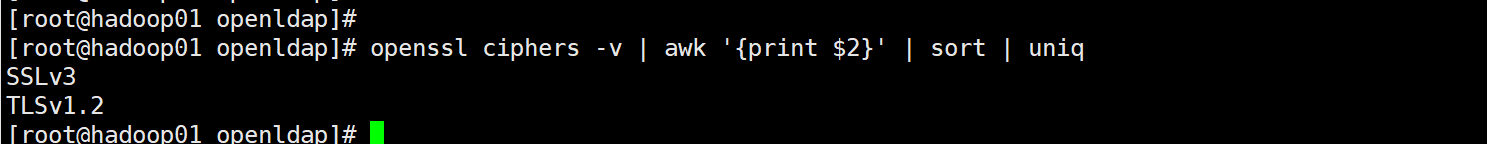
确认LDAP已经开启了TLS



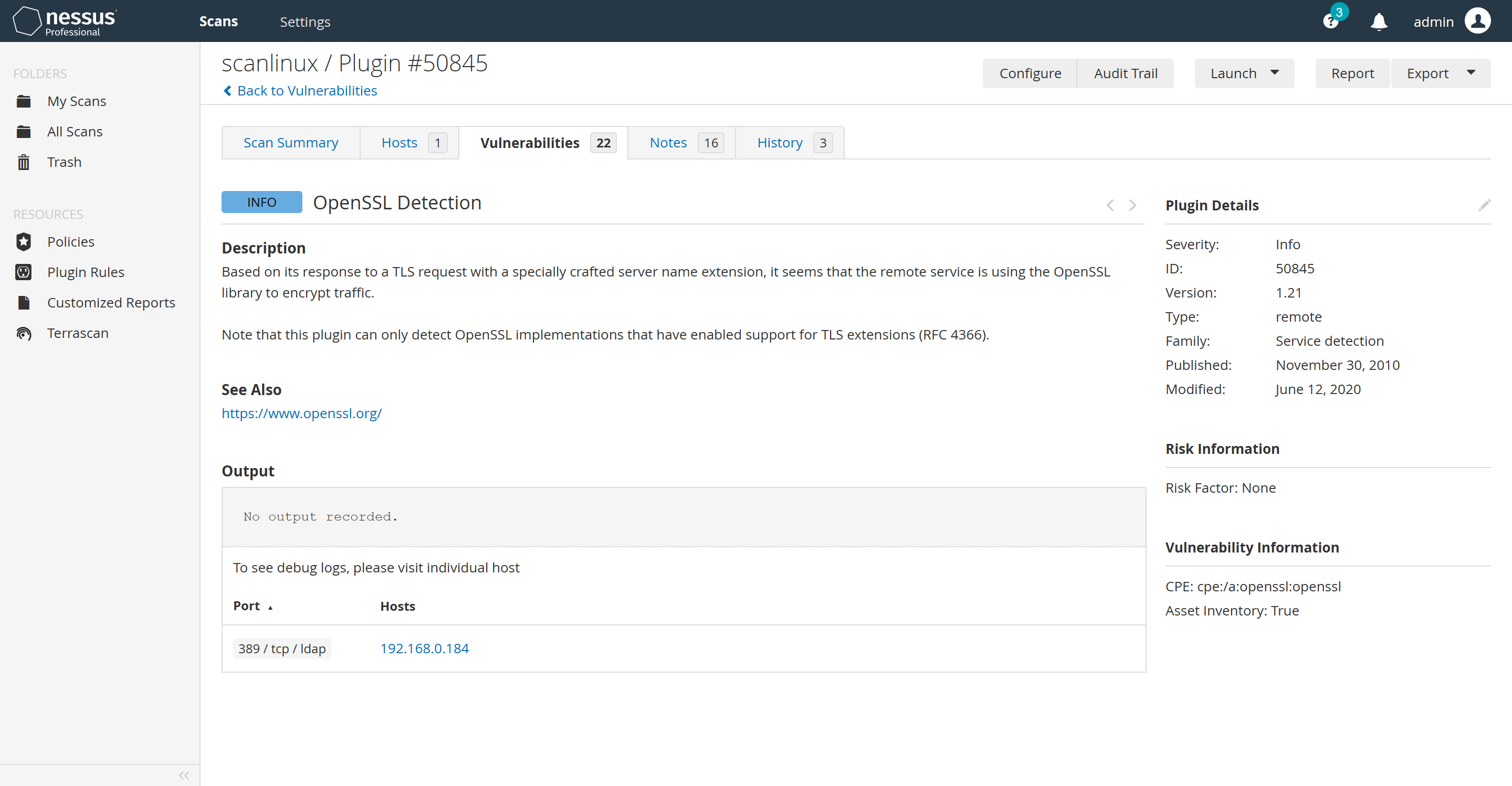
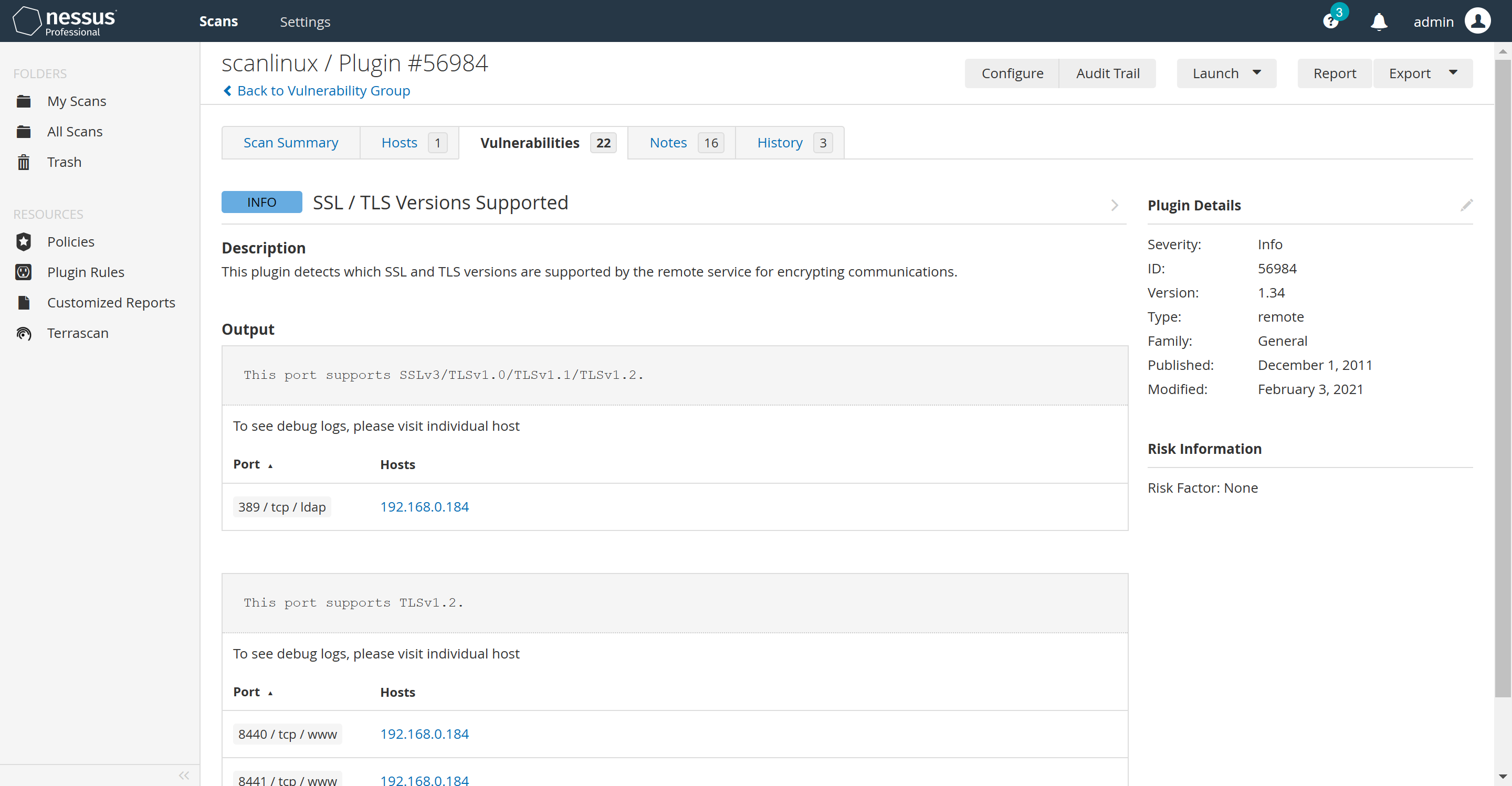
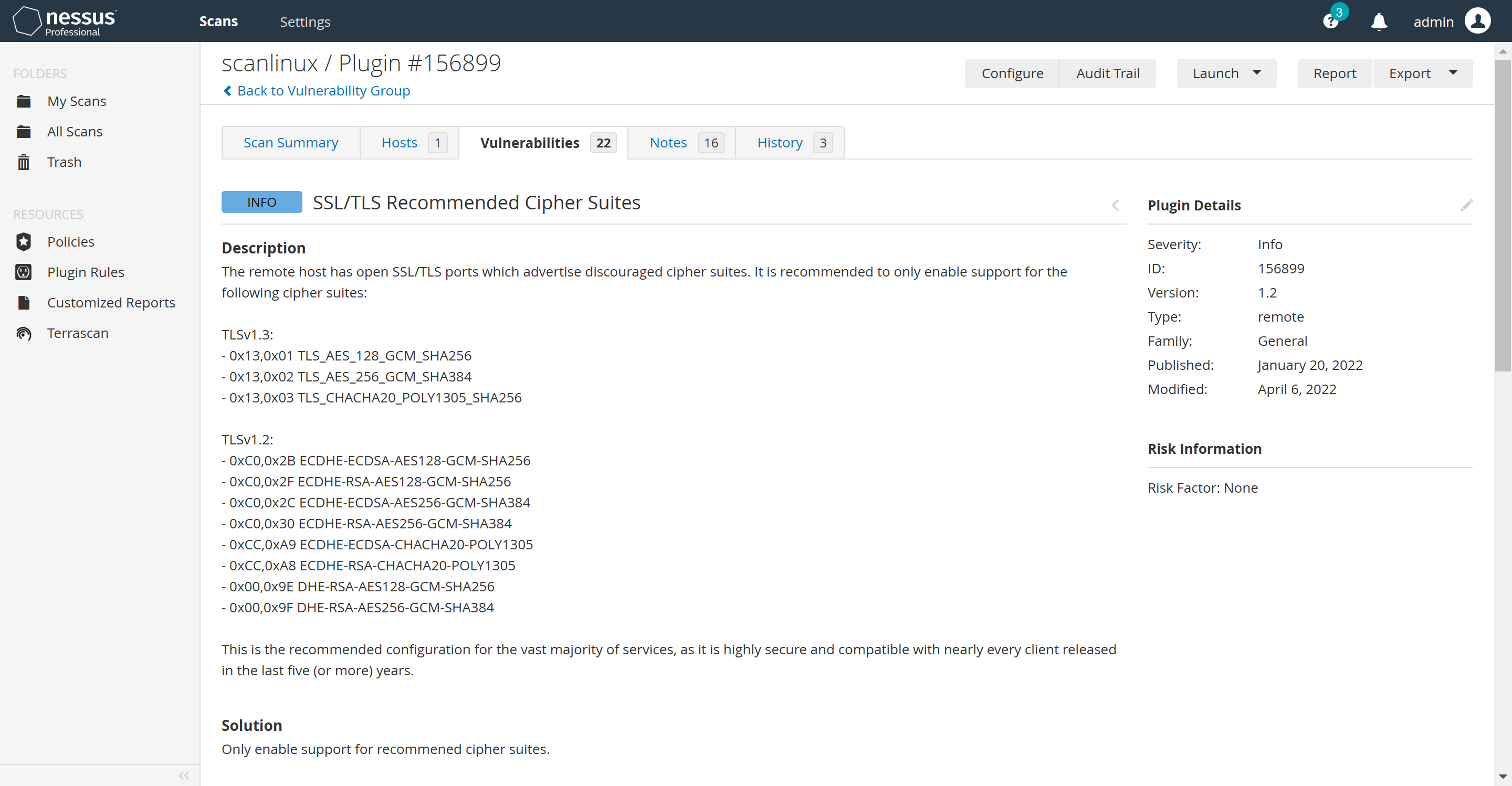
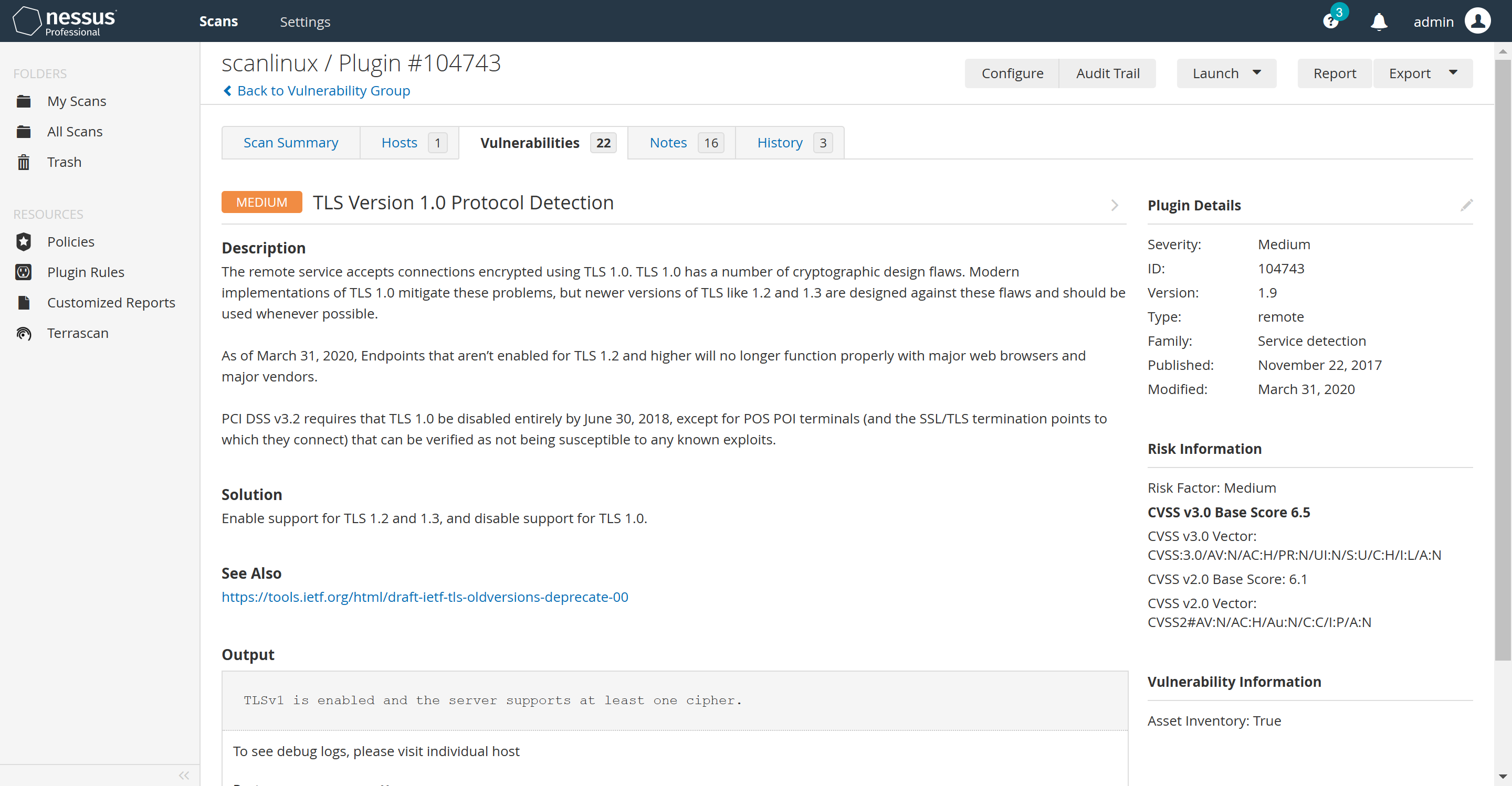
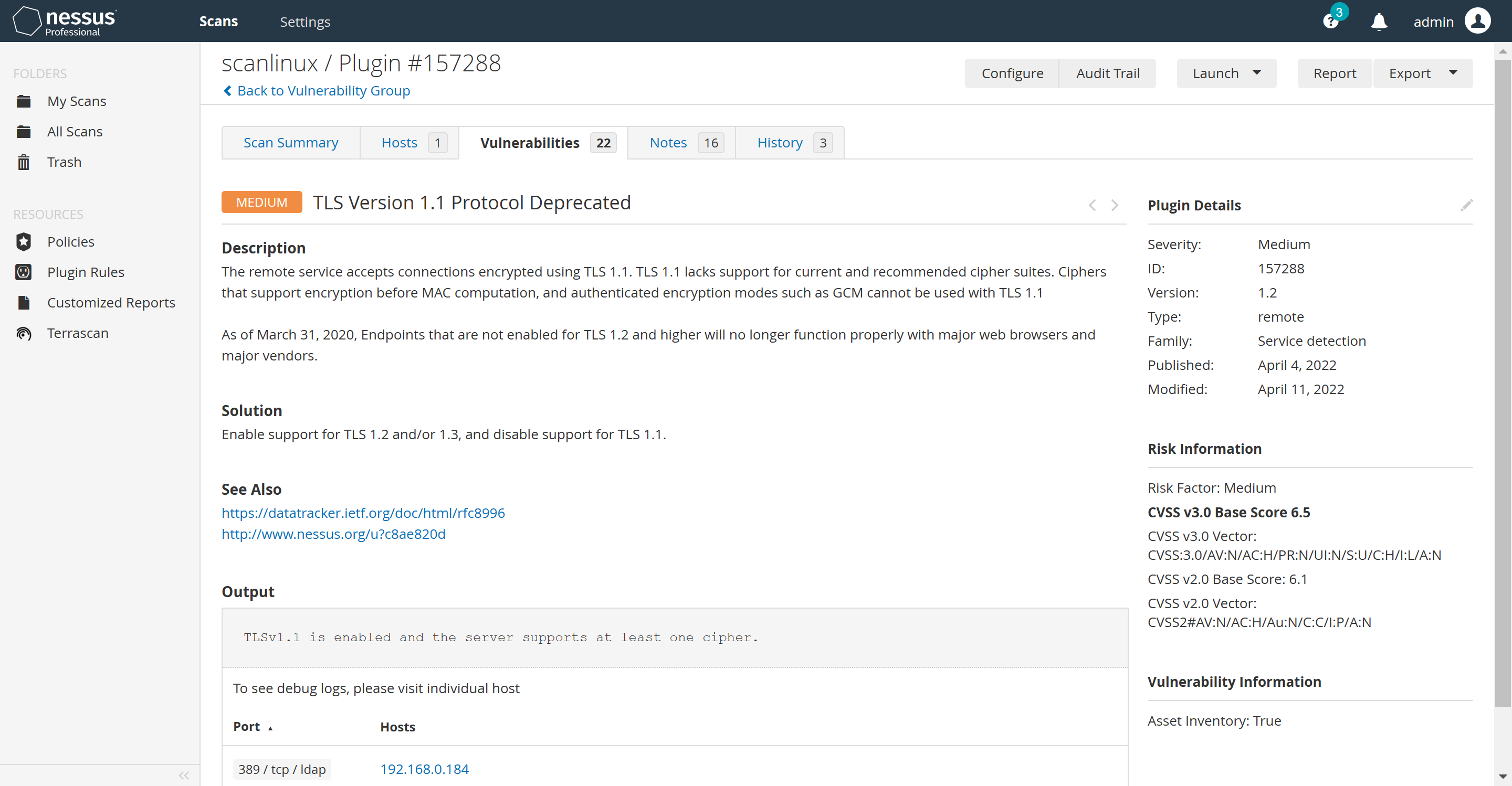
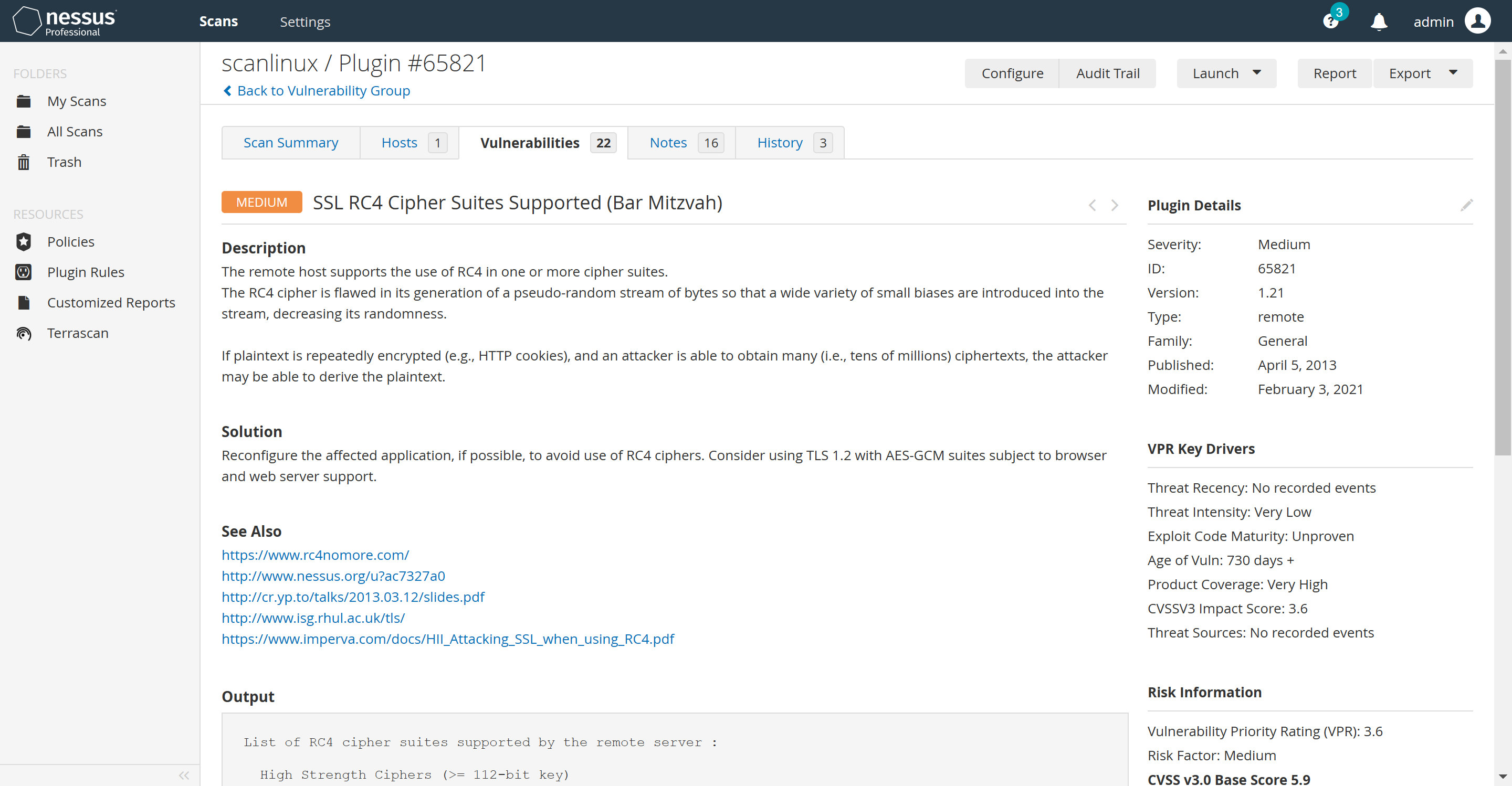


可以查到数据了。

确认当前openssl加密工具包支持的协议版本



使用Nessus扫描漏洞：

TLS Version 1.0 Protocol Detection漏洞

TLS Version 1.1 Protocol Deprecated漏洞

SSL RC4 Cipher Suites Supported (Bar Mitzvah)漏洞修复方法：

手动配置LDAP不支持用SSLv2.0、SSLv3.0、TLS1.0、TLS1.1、RC4算法。

vim tls1.2.ldif

dn: cn=config

changetype: modify

add: olcTLSProtocolMin

olcTLSProtocolMin: 3.3

dn: cn=config

changetype: modify

add: olcTLSCipherSuite

olcTLSCipherSuite: ECDHE-RSA-AES256-SHA384:AES256-SHA256:!RC4:HIGH:!MD5:!aNULL:!EDH:!EXP:!SSLV2:!SSLv3:!TLSv1:!TLSv1.1:!eNULL

dn: cn=config

changetype: modify

add: olcTLSDHParamFile

olcTLSDHParamFile: /etc/openldap/certs/slapd.dh.params

olcTLSProtocolMin: 3.3 支持TLSv1.2或更高版本

olcTLSCipherSuite: ECDHE-RSA-AES256-SHA384:AES256-SHA256:!RC4:HIGH:!MD5:!aNULL:!EDH:!EXP:!SSLV2:!SSLv3:!TLSv1:!TLSv1.1:!eNULL 仅提供最强可用密码

创建DH参数文件

openssl dhparam -out /etc/openldap/certs/slapd.dh.params.tmp 1024

mv /etc/openldap/certs/slapd.dh.params.tmp /etc/openldap/certs/slapd.dh.params

通过确保有一个可用的Diffie-Helman参数文件，可以启用更强的密码。这个密码应该每一段时间(每周)更新一次。

使用ldapmodify命令导入配置到/etc/openldap/slapd.d/cn=config.ldif文件中

ldapmodify -Y EXTERNAL -H ldapi:/// -f tls1.2.ldif

使用TLS=required配置OpenLDAP

vim force-ssl.ldif

dn: olcDatabase={2}hdb,cn=config

changetype: modify

add: olcSecurity

olcSecurity: tls=1

ldapmodify -v -Y EXTERNAL -H ldapi:/// -f force-ssl.ldif

重启slapd

systemctl restart slapd

systemctl status slapd