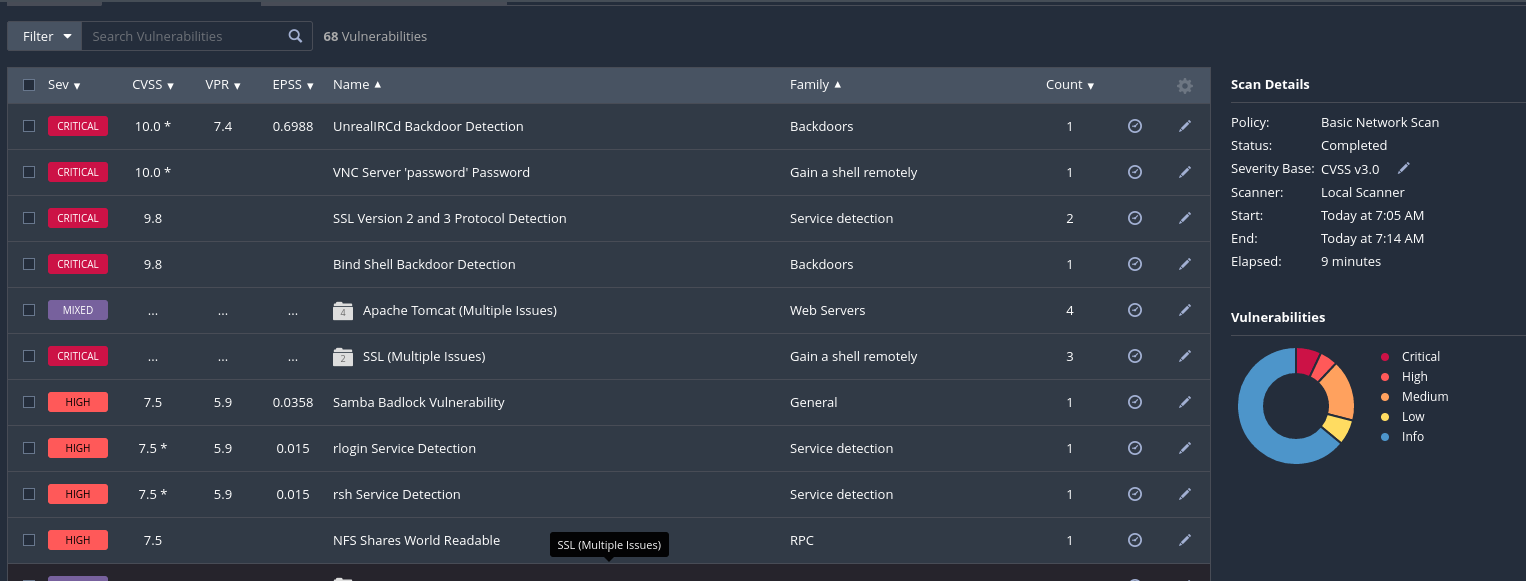
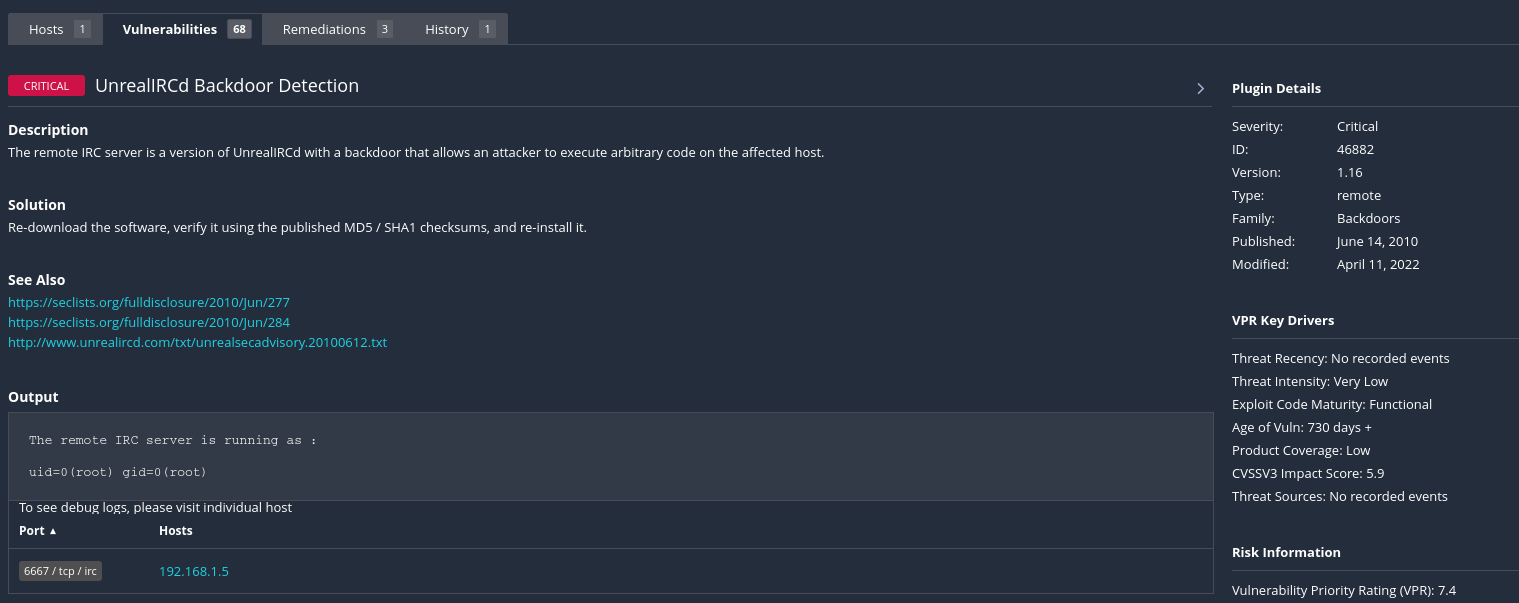
**NESSUS: VULNERABILITY SCANNER**

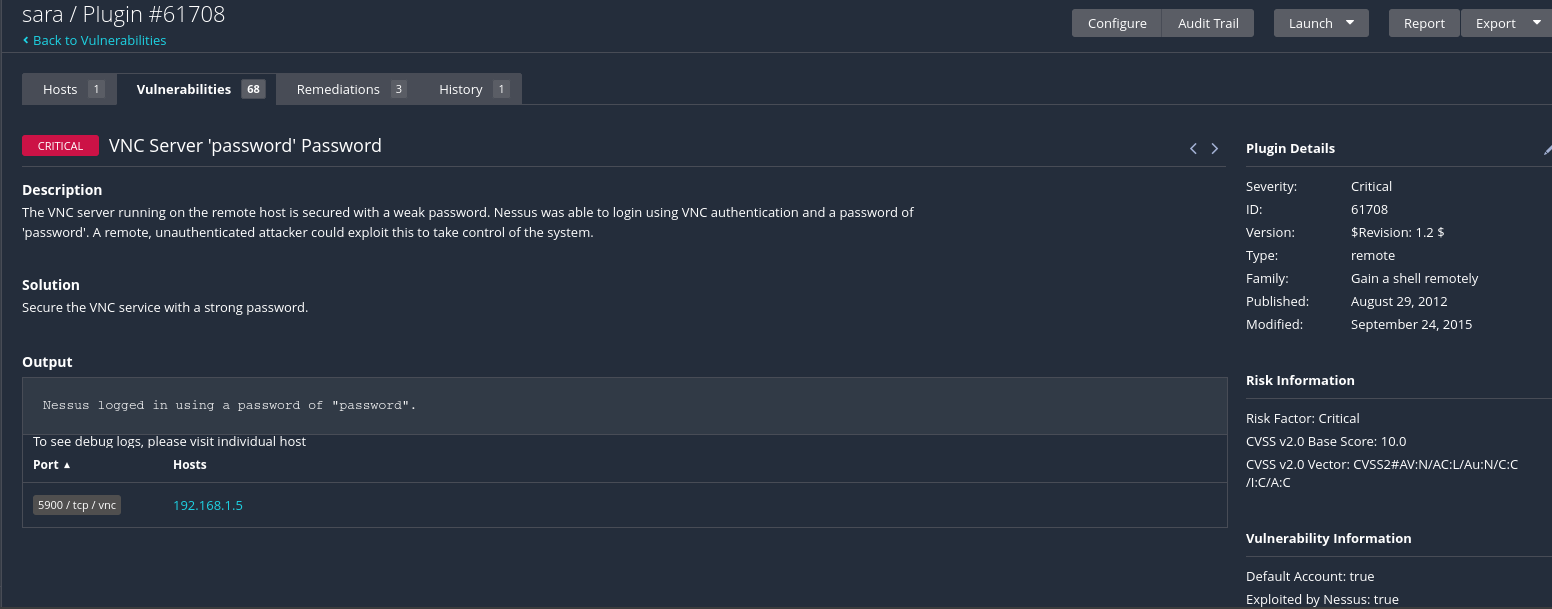


Dopo aver eseguito una scansione dell’host 192.168.1.5 sono emerse delle vulnerabilità delle quali ne esamineremo cinque:

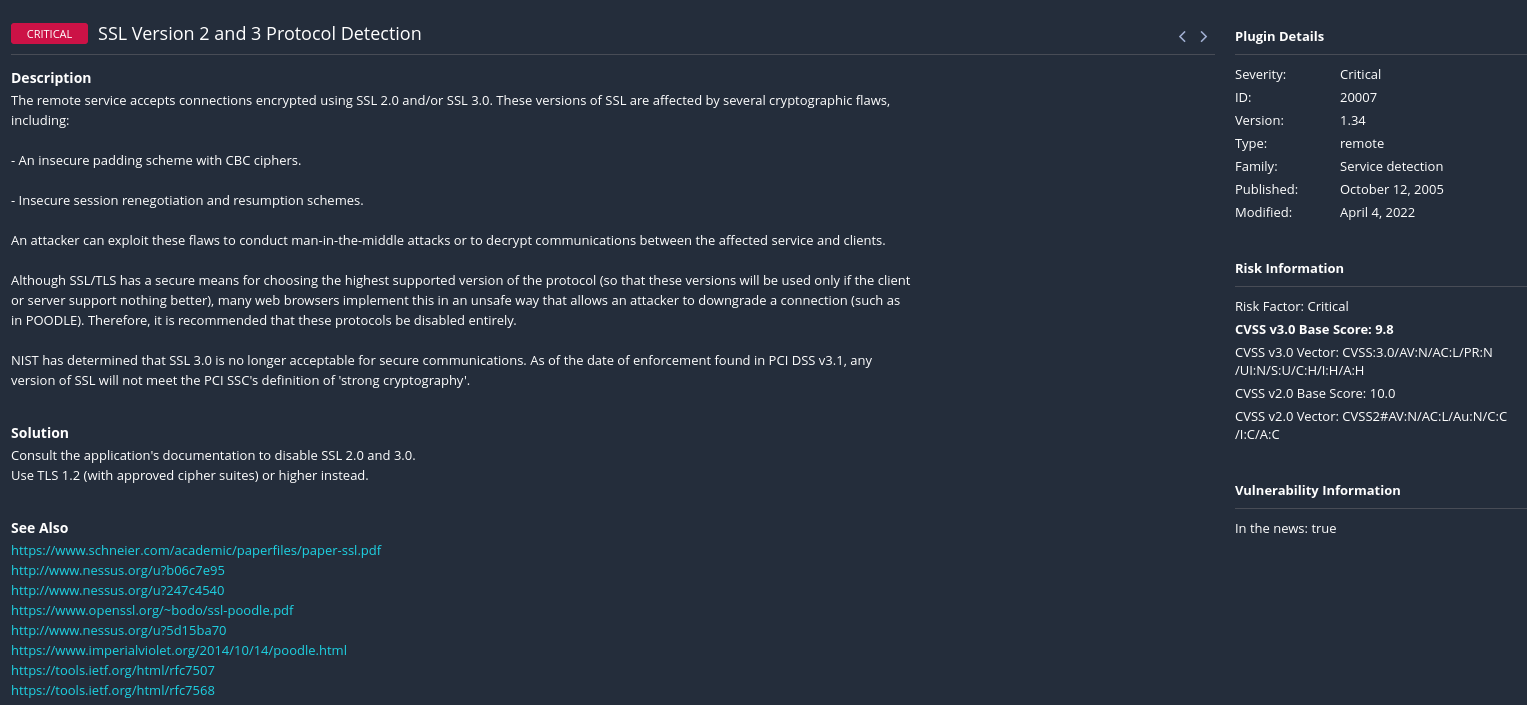
* **UnrealIRCd Backdoor Detection:** Questo può dare a chi attacca un controllo non autorizzato sul sistema.



* **VNC Server 'password' Password :** Questo avviso indica che utilizza una password predefinita molto debole, come "password". Ciò rende facile per gli attaccanti accedere al server e controllare la macchina da remoto.



### **SSL Version 2 and 3 Protocol Detection :** L’uso dei protocolli SSL v2 e v3 è considerato insicuro poiché sono vulnerabili a vari tipi di attacchi. Utilizzarli può esporre i dati trasmessi a intercettazioni e manipolazioni.



### **Bind Shell Backdoor Detection:** Una bind shell è una backdoor che ascolta su una porta aperta, consentendo a un attaccante di connettersi ed eseguire comandi da remoto, mettendo a rischio l’intero sistema.

### 

### **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness:** significa che le chiavi potrebbero essere prevedibili, facilitando l’accesso non autorizzato al sistema.

