| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME |
|---|---|---|---|---|---|
| CRITICAL | 9.8 | 8.9 | 0.9447 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | - | - | 51988 | Bind Shell Backdoor Detection |
| CRITICAL | 9.8 | - | - | 20007 | SSL Version 2 and 3 Protocol Detection |
| CRITICAL | 10.0 | - | - | 201352 | Canonical Ubuntu Linux SEoL (8.04.x) |
| CRITICAL | 10.0* | 5.1 | 0.0165 | 32314 | Debian OpenSSH/OpenSSL Package Random Number Genera Weakness |
| CRITICAL | 10.0* | 5.1 | 0.0165 | 32321 | Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check) |
| CRITICAL | 10.0* | - | - | 61708 | VNC Server 'password' Password |

Dopo vari tentativi che adesso vi andrò ad elencare le criticità si ripropongono sempre e quindi non sono riuscito a fixare nulla.

1. Bind Shell Backdoor Detection
   netstat -tulnp | grep LISTEN (identifichiamo la porta sospetta tramite questo comando) la porta che mi ha piu insospettito è la 3632 che è la porta piu usata per gli exploit da remoto.
   Identifichiamo il PID della porta tramite questo comando: sudo netstat -tulnp | grep :3632 e vediamo che il PID è uguale a 4236. Terminiamo il processo tramite sudo kill -9 4236. Verifichiamo che la porta sia chiusa utilizzando il codice: netstat -tulnp | grep :3632 e se non appare nulla la porta è libera ed il processo è stato terminato correttamente.
2. VNC Server ‘password’ Password
   which vncpasswd usiamo questo comando per vedere se vncpasswd è presente sulla macchina, avviamolo tramite il codice vncpasswd, scegliamo e confermiamo la nuova password ed in fine verifichiamo che il file sia stato aggiornato scrivendo: ls -l ~/.vnc/passwd. Killiamo il server (vncserver -kill :1) e riavviamolo (vncserver :1).