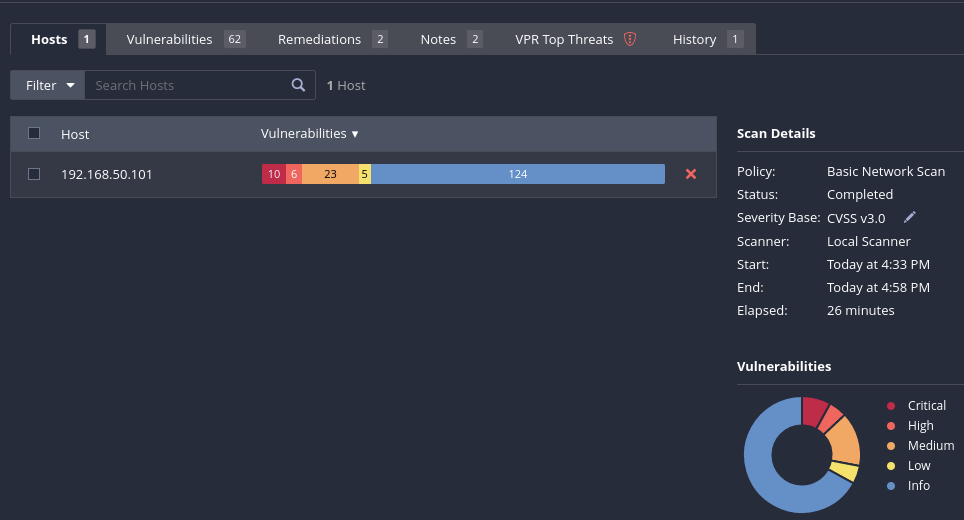
**VULNERABILITY ASSESSMENT**

*Vulnerability scanner: Nessus*

*Target: Metasploitable - 192.168.50.101*

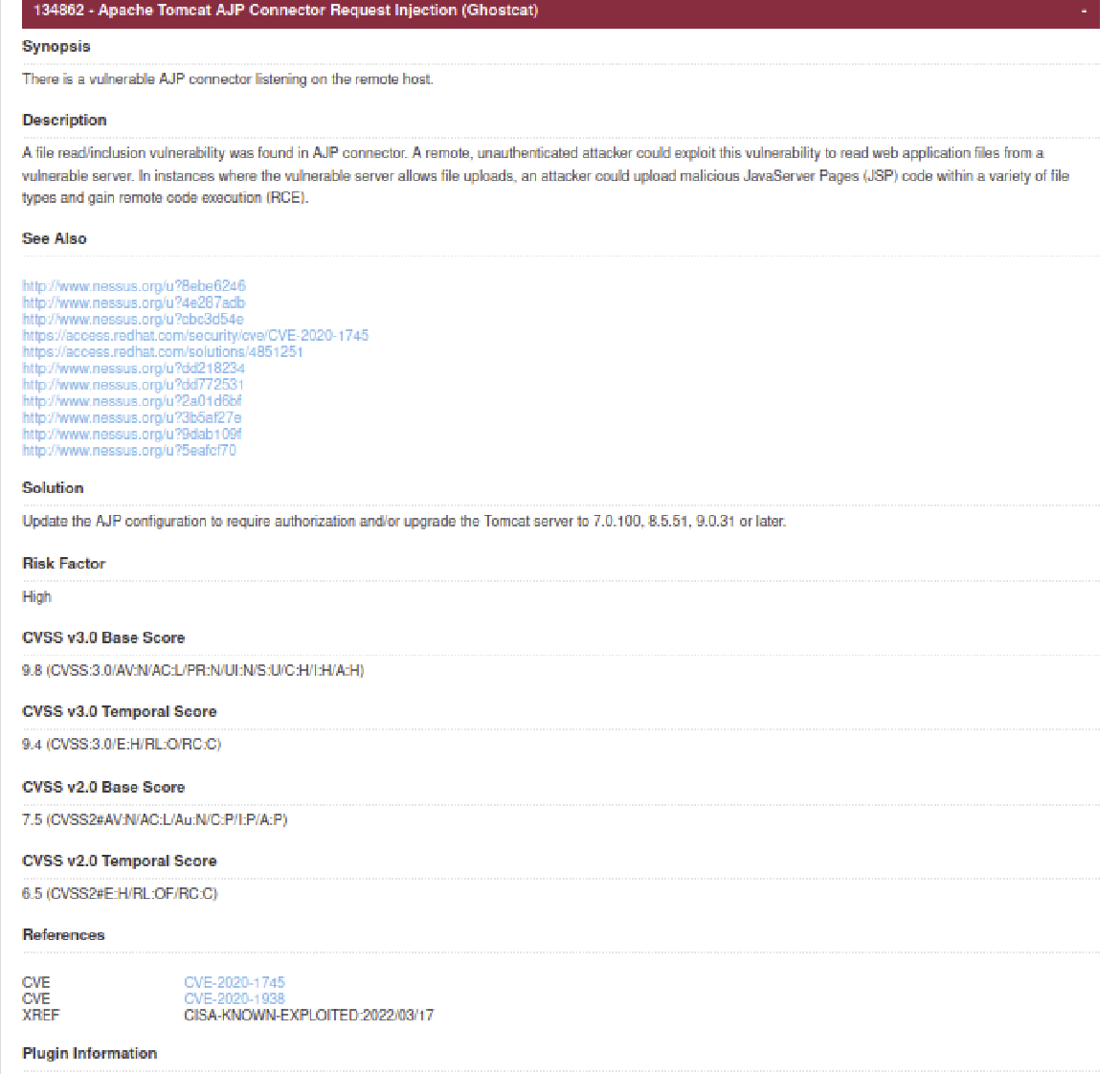
*Spett.le Azienda,*

*a seguito vostra richiesta d’intervento sulla verifica di eventuali vulnerabilità sulla vostra rete abbiamo riscontrato quanto diverse criticità. Qui di seguito un report della scansione effettuata sull’ip in intestazione*

1. *Il primo passo è stato di effettuare una scansione sulle porte di rete comuni(1-1024). Cosi facendo, applicando un “basic network scan” abbiamo effettivamente riscontrato diverse vulnerabilità. D’importante evidenza sono quelle “critiche” rappresentati nei grafici sotto riportati.*

*Come potete notare dal grafico, 16 di esse rappresentano delle criticità importanti.*

*La prima criticità riscontrata è relativa alla vulnerabilità AJP.*

*L’AJP è un connettore che mette in collegamento l’Application server nel backend con il frontend ( Questi ultimi due definiscono la struttura del sito con tutti loro “crismi”) ,eseguendo l’interfaccia grafica del sito e rimandando al frontend il contenuto sotto forma di HTML/JS che verrà infine renderizzato per il browser dell’utente fi**nale.*

*Qualora avvenisse un attacco , il criminal hacker potrebbe avere la possibilità di caricare ed eseguire diversi codici di script, tali da falsare in maniera inappropriata i contenuti del vostro servizio.*

*La soluzione trovata e quindi altamente suggerita è di riconfigurare l’AJP, ed eseguire un upgrade all’Application sever Tomcat.*

*upgrade suggeritI: 7.0.100. - 8.5.51. - 9.0.31 o più recenti*

*Per ulteriori approfondimenti a riguardo della criticità riscontrata, riportiamo qui di seguito un link utile: <https://www.dell.com/support/kbdoc/it-it/000020741/cve-2020-1938>*