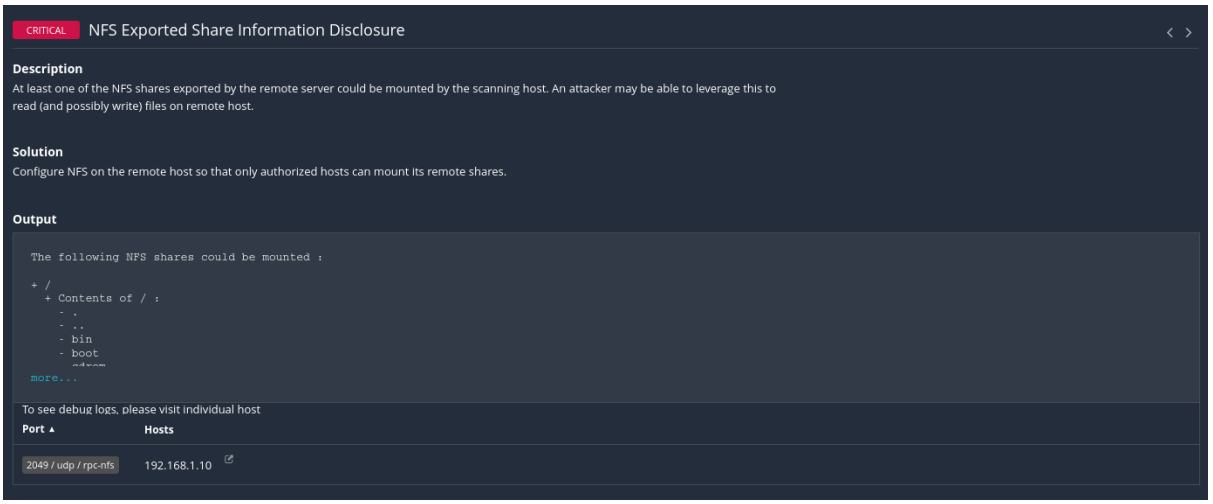
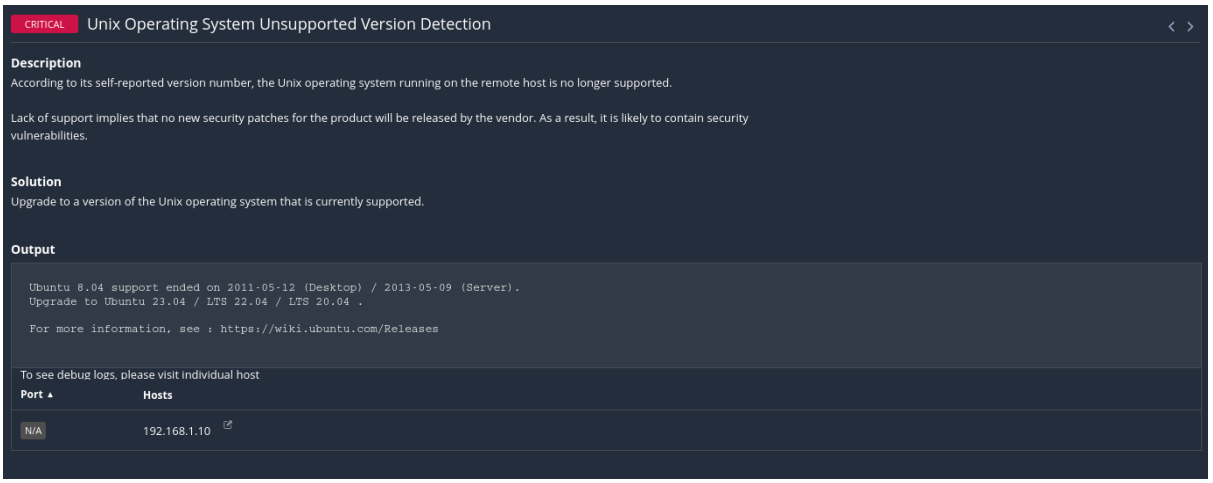
La prima vulnerabilità



consente a un utente non autorizzato di accedere alle condivisioni NFS di un host remoto. Infatti, tale utente potrebbe sfruttare questa vulnerabilità per accedere a file sensibili o dati riservati. Si potrebbe anche utilizzare la vulnerabilità per ottenere un accesso privilegiato all'host remoto.
Per risolvere questa vulnerabilità, è necessario configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le condivisioni NFS remote.
In alternativa, è possibile utilizzare un firewall per bloccare l'accesso alle condivisioni NFS da parte di host non autorizzati.

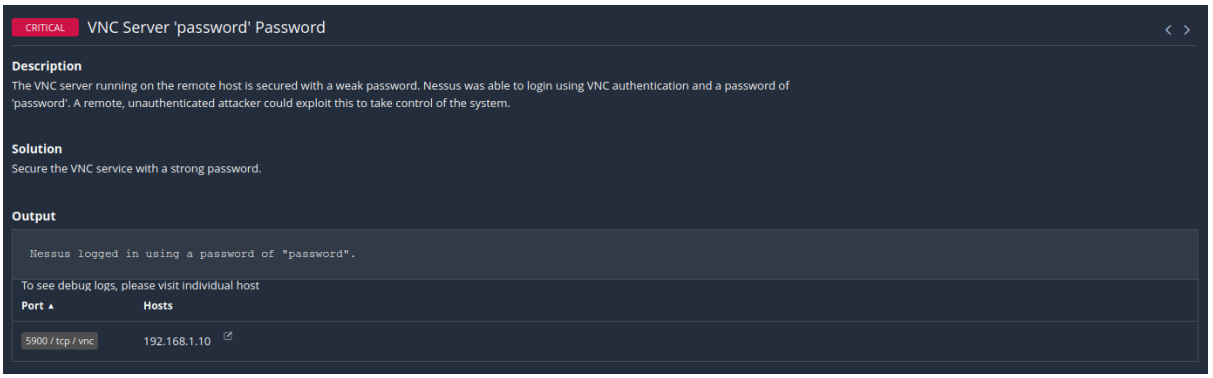
La seconda vulnerabilità



riguarda la versione non supportata del sistema operativo Unix. Ciò significa che il sistema operativo in esecuzione sull'host remoto non è più supportato dal fornitore. La mancanza di supporto implica che il

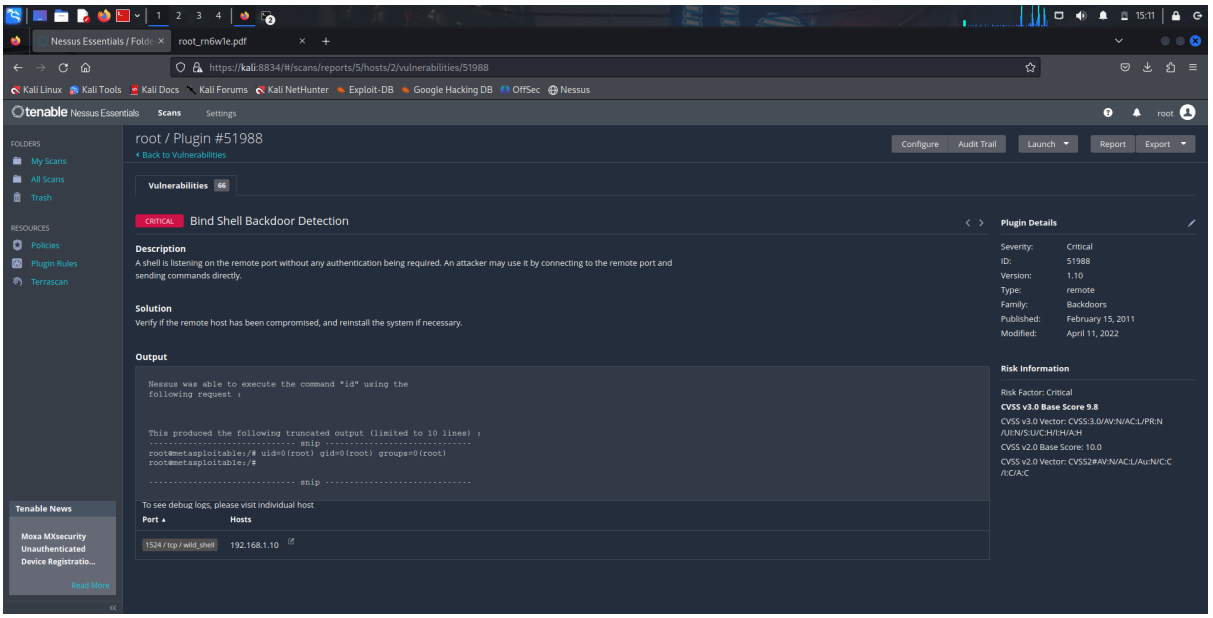
fornitore non rilascerà più patch di sicurezza per il prodotto. Di conseguenza, è probabile che il sistema operativo contenga vulnerabilità di sicurezza note.
Nello specifico, la vulnerabilità trovata rileva le versioni non supportate del sistema operativo Unix. In questo caso, il sistema operativo in esecuzione sull'host remoto è una versione di Debian 8.0, che è stata rilasciata nel 2015. Debian ha smesso di supportare questa versione nel 2017.
La soluzione a questa vulnerabilità è aggiornare il sistema operativo a una versione attualmente supportata. Nel caso di Debian, la versione attualmente supportata è Debian 11.

La terza vulnerabilità



identifica una password debole in un server VCN. Questa vulnerabilità consente ad un utente malintenzionato di accedere al server VCN senza alcuna autenticazione e controllarlo da remoto.
Il rapporto di Nessus indica che la password è "password". Questa password è ovviamente debole.
La vulnerabilità è stata pubblicata per la prima volta nel 2012 ed è stata risolta nel 2015. Tuttavia, è possibile che alcuni server VCN non siano stati aggiornati alla versione più recente.
Per correggere questa vulnerabilità, è necessario aggiornare il server VCN alla versione più recente o modificare la password utilizzandone una più forte.

La quarta vulnerabilità



è una porta di shell bind in ascolto su una porta remota senza alcuna autenticazione richiesta. Ciò significa che un utente malintenzionato può connettersi alla porta remota ed eseguire qualsiasi comando desiderato. Per correggere la vulnerabilità, è necessario disabilitare la porta di shell bind. Ciò può essere fatto modificando la configurazione del servizio che sta in ascolto sulla porta.