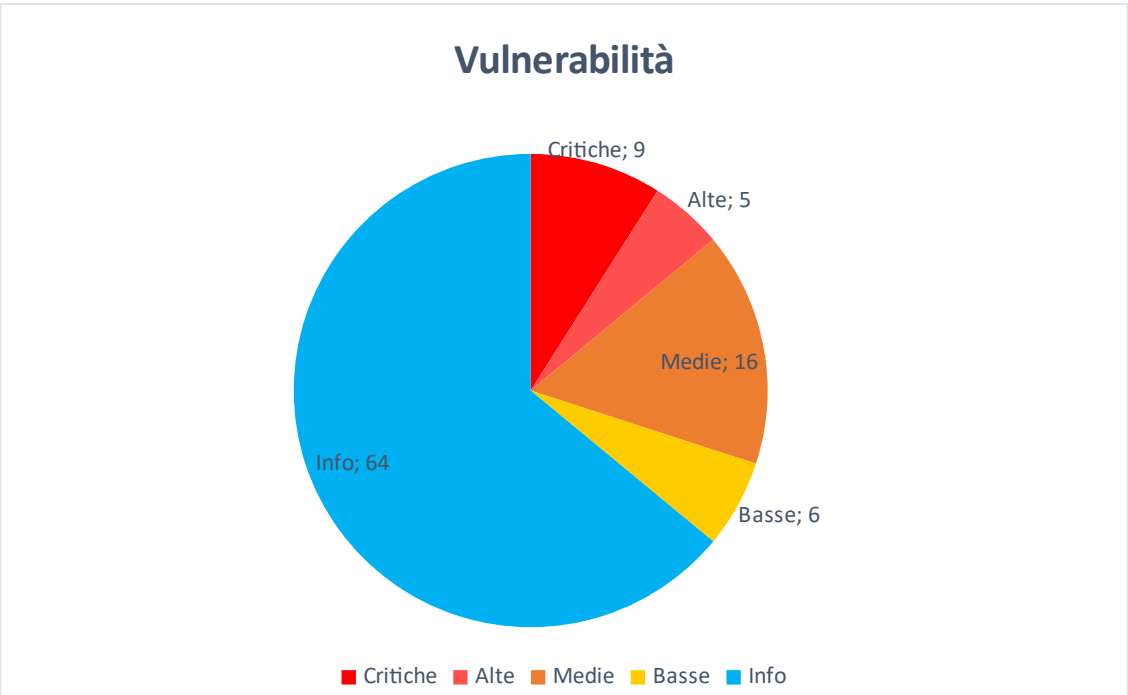
Scansione Inizio

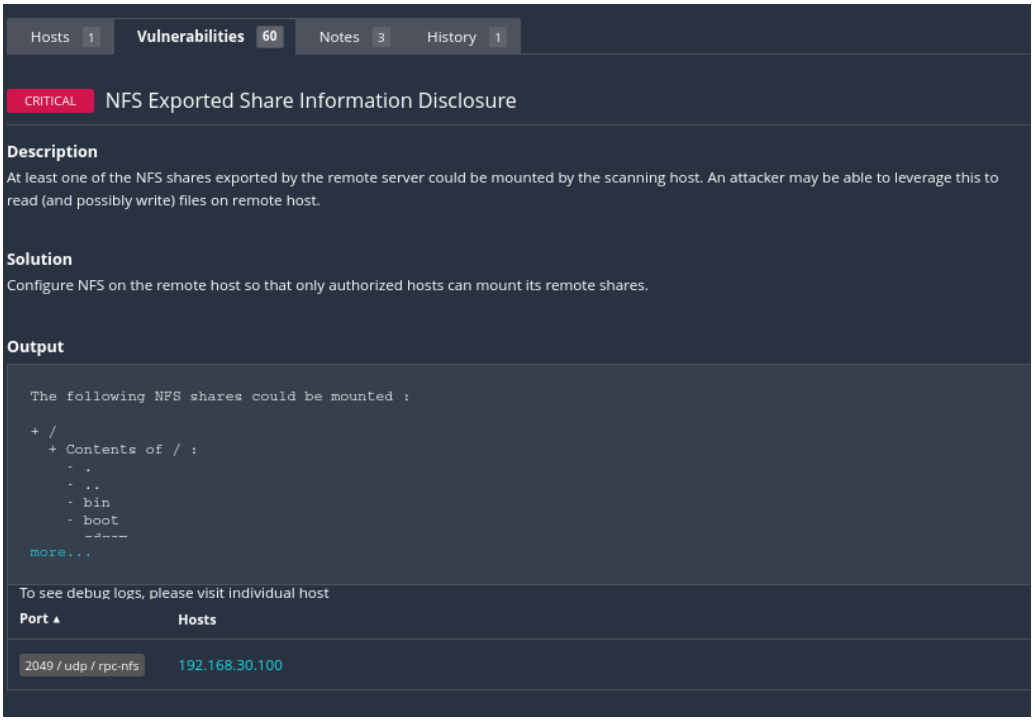
Hosts 1 | **Vulnerabilities 68** | Remediations 3 | Notes 3 | History 17

Filter | Search Vulnerabilities | 68 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	...	SSL (Multiple Issues)	Service detection	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MIXED	...	...	SSH (Multiple Issues)	Misc.	6

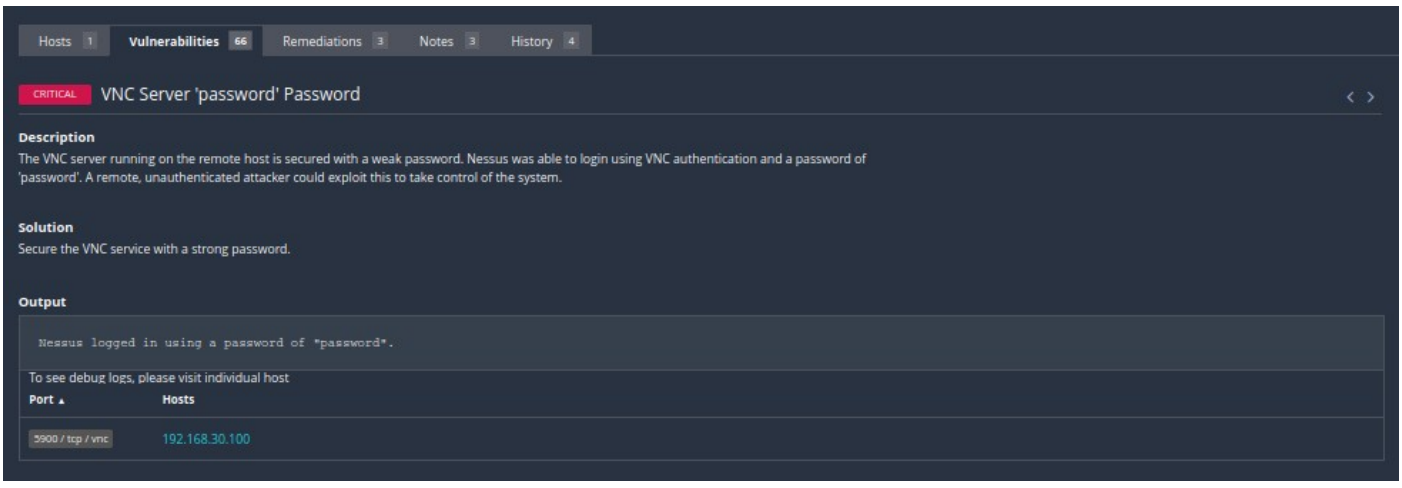


NFS Export Share Information Disclosure



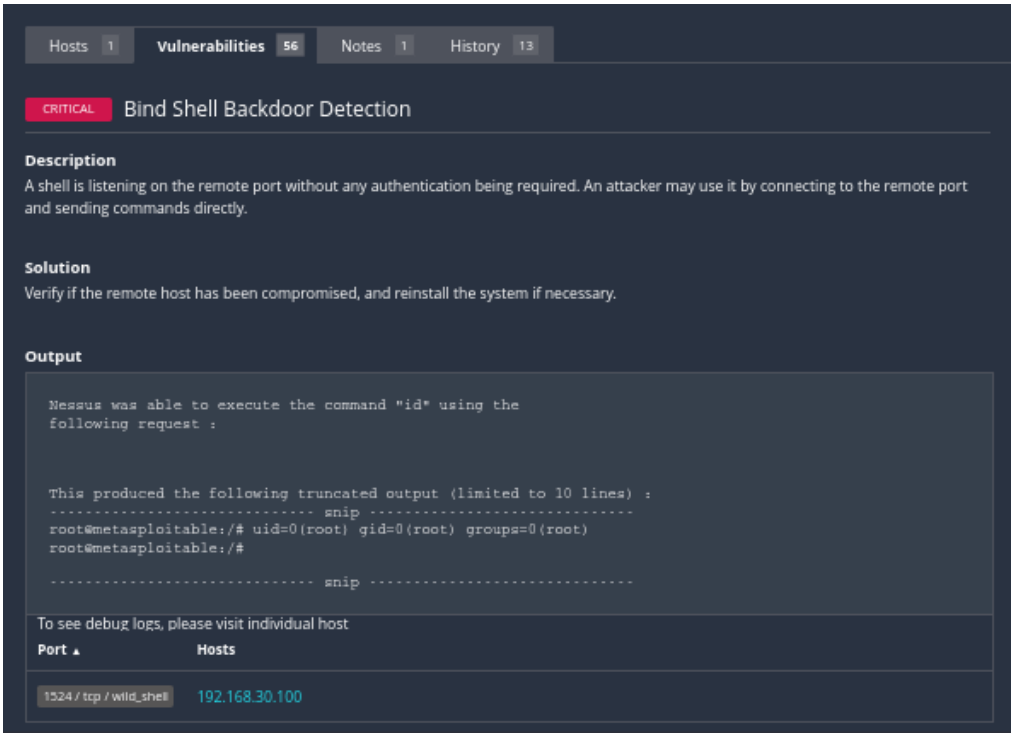
NFS = Network File System è un protocollo di sistema, che consente ai clienti di accedere a file e directory su una reta, questo vuol dire che sono accessibili da remoto. Se gli NFS non sono protetti correttamente c'è la possibilità che terze parti possano accedere a queste informazioni; modificandole o eventualmente divulgarle.

VNC Server 'password' Password



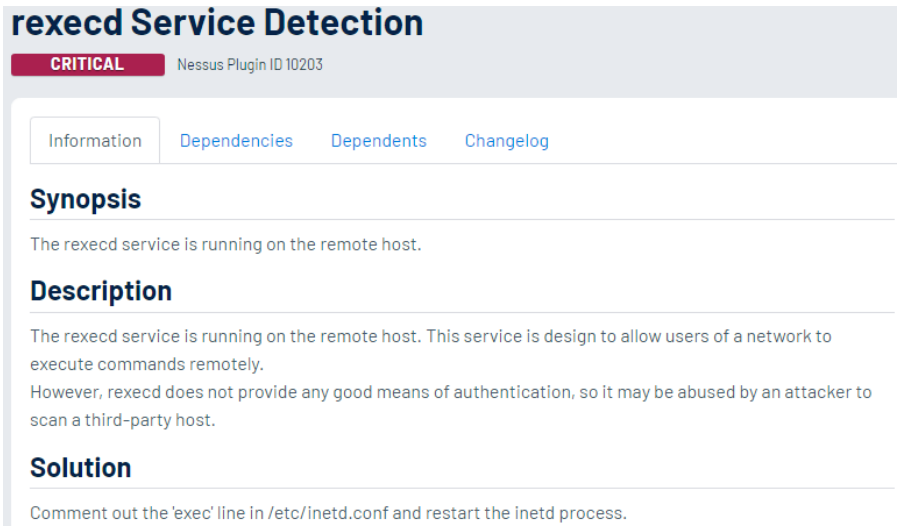
VNC= Virtual Network Computing è un protocollo che consente a un utente di controllare un computer da remoto. Nessus consiglia di cambiare la password attuale con una più complessa.

Bind Shell Backdoor Detection



Una Shell è in ascolto su una porta (la 1524) remota senza autenticazione. Questa può essere utilizzata da un attaccante che può collegarsi e inviare comandi da remoto.

Rexecd Service Detection



Il servizio Rexecd è progettato per consentire agli utenti di una rete di eseguire comandi in remoto su un sistema. Tuttavia, è importante notare che Rexecd non fornisce un mezzo di autenticazione adeguato, il che significa che potrebbe essere abusato da un attaccante per eseguire comandi non autorizzati su un sistema di terze parti o per effettuare scansioni indesiderate su altre macchine.