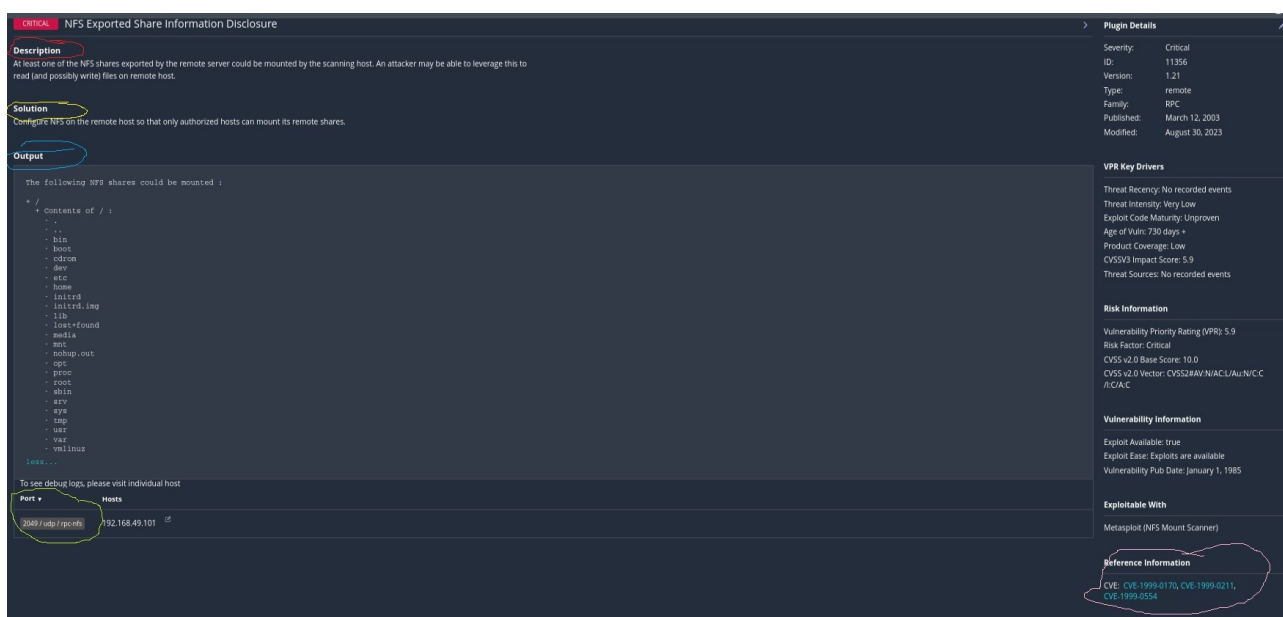


Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1
HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1
HIGH	7.5		NFS Shares World Readable	RPC	1
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

Dalla scansione dell' ip 192.168.49.101 che corrisponde a metasploitable usando nessus si evincono svariate vulnerabilita' suddivise per criticita' di cvss, in ordine decrescente di gravita'



CRITICAL NFS Exported Share Information Disclosure

Description
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output
The following NFS shares could be mounted :

```

+ /
+ Contents of / :
+ ..
+ .
+ bin
+ boot
+ cdrom
+ dev
+ etc
+ home
+ initrd
+ initrd.img
+ lib
+ lost+found
+ media
+ mnt
+ mnt/cp
+ opt
+ proc
+ root
+ sbin
+ srv
+ sys
+ tmp
+ usr
+ var
+ vmlinuz
+ ...

```

Port 2049 /udp /tcp
Hosts 192.168.49.101

Plugin Details
Severity: Critical
ID: 11356
Version: 1.21
Type: remote
Family: RPC
Published: March 12, 2003
Modified: August 30, 2023

VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSv3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information
Vulnerability Priority Rating (VPR): 5.9
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/R:C/A:C

Vulnerability Information
Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: January 1, 1985

Exploitable With
Metasploit (NFS Mount Scanner)

Reference Information
CVE: CVE-1999-0176, CVE-1999-0211, CVE-1999-0554

prendendo ad esempio la prima criticita' nella lista,

- essa ci mostra una descrizione del tipo di vulnerabilita' (evidenziata in rosso nell'immagine) che dice che alcuni file condivisi dal protocollo nfs al server possono essere sfruttati per connettersi da remoto a metasploitable;
- nella parte in giallo c'è una possibile soluzione da attuare, in questo caso si tratta di modificare le impostazioni dell'nfs in modo tale che solo gli autorizzati possano usare il controllo da remoto;
- nella parte evidenziata in blu viene fatto l'elenco dei file condivisi dallo nfs che possono essere sfruttati;
- nella parte in verde in basso a sinistra viene scritto il numero della porta che ha questa vulnerabilita' e i vari protocolli usati, porta 2049 e tcp o udp;
- nella parte in rosa in basso a destra ci sono delle fonti esterne da cui poter trarre ulteriori informazioni