

Remediation

Vulnerability: NFS Exported Share Information Disclosure

Soluzione:

Come possiamo quindi prevenire gli attacchi a questa vulnerabilità?

Innanzitutto, posso limitare l'accesso. Posso specificare indirizzi IP o subnet specifici a cui è consentito accedere alle condivisioni NFS. Posso farlo sul file `/etc/exports` in metasploitable.

```
msfadmin@metasploitable:~$ sudo nano /etc/exports_
```



Quindi posso digitare gli indirizzi IP o le subnet che desidero nell'editor di testo.

```
GNU nano 2.0.7      File: /etc/exports

# /etc/exports: the access control list for filesystems which may be exported
#                 to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/      192.168.50.120(rw,sync,no_root_squash,no_subtree_check)

[ Read 12 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

Posso configurare le regole del firewall come un altro metodo.

Posso impostare le regole del firewall per consentire solo il traffico NFS necessario.

Ad esempio, posso usare *ufw* .

```
msfadmin@metasploitable:~$ sudo ufw allow from 192.168.50.120 to any port 2049
Rules updated
msfadmin@metasploitable:~$ _
```

Vulnerability: Bind Shell Backdoor Detection

Ho tentato di chiudere questa porta usando il comando fuser.

```
-a      display unused files too
-c      mounted FS
-f      silently ignored (for POSIX compatibility)
-i      ask before killing (ignored without -k)
-k      kill processes accessing the named file
-l      list available signal names
-m      show all processes using the named filesystems
-n SPACE search in this name space (file, udp, or tcp)
-s      silent operation
-SIGNAL send this signal instead of SIGKILL
-u      display user IDs
-v      verbose output
-V      display version information
-4      search IPv4 sockets only
-6      search IPv6 sockets only
-       reset options

udp/tcp names: [local_port][,[rmt_host][,[rmt_port]]]

msfadmin@metasploitable:~$ sudo fuser -k -n tcp 1524
[sudo] password for msfadmin:
1524/tcp:      4509
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

- -k = uccide il processo
- -n = id processo