

## NFS Shares World Readable:

La condivisione NFS era configurata in modo che tutti gli utenti potesse leggere i dati.

HIGH

NFS Shares World Readable

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

Solution

Place the appropriate restrictions on all NFS shares.

See Also

<http://www.tldp.org/HOWTO/NFS-HOWTO/security.html>

Output

The following shares have no access restrictions :  
/ \*  
To see debug logs, please visit individual host

Port	Hosts
2049 /tcp /rpcnfs	192.168.1.144

Plugin Details

Severity: High  
ID: 42256  
Version: 1.11  
Type: remote  
Family: RPC  
Published: October 26, 2009  
Modified: May 5, 2020

Risk Information

Risk Factor: Medium  
CVSS v3.0 Base Score 7.5  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N  
CVSS v2.0 Base Score: 5.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Vulnerability Information

Vulnerability Pub Date: January 1, 1985

La configurazione NFS è stata modificata in modo da limitare l'accesso solo agli host autorizzati, aggiungendo indirizzi IP specifici alle esportazioni NFS. (La soluzione di NFS Exported Share Information ha permesso di ridurre il rischio anche di questa vulnerabilità)

## rlogin Service Detection:

Il servizio rlogin era attivo, esponendo il sistema a potenziali rischi di sicurezza.

HIGH

rlogin Service Detection

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Output

No output recorded.  
To see debug logs, please visit individual host

Port	Hosts
513 /tcp /rlogin	192.168.1.144

Plugin Details

Severity: High  
ID: 10205  
Version: 1.36  
Type: remote  
Family: Service detection  
Published: August 30, 1999  
Modified: April 11, 2022

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): 6.7

Il servizio rlogin è stato disabilitato commentando la linea nel file di login.

```
meta [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/inetd.conf      Modified
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.tftpd
telnet                  stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.tftpd
ftp                    dgram   udp      wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd
shell                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
rlogin                 stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec                   stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
pingreslock stream tcp nowait root /bin/bash bash -i
```

## VNC Server 'password' Password:

Il server VNC utilizzava una password debole ('password').

CRITICAL

VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

Nessus logged in using a password of "password".

To see debug logs, please visit individual host

Port

Hosts

5900 / tcp / vnc

192.168.1.144

Plugin Details

Severity: Critical

ID: 61708

Version: \$Revision: 1.2 \$

Type: remote

Family: Gain a shell remotely

Published: August 29, 2012

Modified: September 24, 2015

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Default Account: true

Exploited by Nessus: true

La password VNC è stata cambiata con una più sicura

meta [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

La macchina virtuale segnala che il sistema guest supporta integrazione del puntatore del mouse. Ciò significa che non è necessario cliccare con il mouse per spostare il cursore. Per saperne di più, visitate [questo sito](#).

msfadmin@metasploitable:~\$ vncpasswd  
Using password file /home/msfadmin/.vnc/passwd  
VNC directory /home/msfadmin/.vnc does not exist, creating.  
Password:  
Verify:  
Would you like to enter a view-only password (y/n)? y  
Password:  
Verify:  
msfadmin@metasploitable:~\$