

## TRACCIA

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure
<input type="checkbox"/>	CRITICAL	10.0 *	rexecd Service Detection
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' Password
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection

Risolviamo solamente i problemi evidenziati in giallo.

## NFS Exported Share Information Disclosure

# NFS Exported Share Information Disclosure

Language: English ▾

**CRITICAL** Nessus Plugin ID 11356

Information

Dependencies

Dependents

Changelog

### Synopsis

It is possible to access NFS shares on the remote host.

### 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.

### Plugin Details

**Severity:** Critical

**ID:** 11356

**File Name:** nfs\_mount.nasl

**Version:** 1.21

**Type:** remote

**Family:** [RPC](#)

**Published:** 3/12/2003

**Updated:** 8/30/2023

**Supported Sensors:** Nessus

Per risolvere questo exploit possiamo aggiornare il sistema applicando la patch jumbo NFS (Patch-ID# 100173-13), disponibile sul sito Web di Sun Microsystems.

## Dettagli

---

nfs-guess (77) **riportato Dec 6, 1991**

Most NFS implementations have specific patterns in their filehandles that can be guessed. Most NFS implementations rely on the secrecy of filehandles for the files' actual security. An attacker can guess filehandles to bypass mountd security and gain unauthorized access to NFS resources and all files on the NFS volume.

## Conseguenze:

---

Gain Access

## Soluzione

---

Apply the NFS jumbo patch (Patch-ID# 100173-13), available from the Sun Microsystems Web site. See References.

After installing the patch, run fsirand on your entire file system. The new fsirand program makes it difficult for a remote system user to guess NFS filehandles, preventing the user from conducting unauthorized mounts and accessing your NFS file systems.

## rexecd Service Detection

# rexecd Service Detection

Language: English ▾

CRITICAL

Nessus Plugin ID 10203

Information

Dependencies

Dependents

Changelog

### Synopsis

The rexecd service is running on the remote host.

### Description

The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely.

However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

### Solution

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

### Plugin Details

**Severity:** Critical

**ID:** 10203

**File Name:** rexecd.nasl

**Version:** 1.33

**Type:** remote

**Family:** [Service detection](#)

**Published:** 8/31/1999

**Updated:** 6/29/2023

**Supported Sensors:**  
Nessus

```
GNU nano 2.0.7      File: etc/inetd.conf      Modified

#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet                stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp                 dgram  udp    wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i

[ Read 8 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
```

```
GNU nano 2.0.7      File: etc/inetd.conf      Modified

#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet                stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp                 dgram  udp    wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
#exec                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i

[ Read 8 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
```

Apri con il comando nano il file inetd.conf che si trova nella directory /etc dall'inizio della directory.  
Puoi raggiungere la directory di avvio usando il comando cd/

## VNC Server 'password' Password

# VNC Server 'password' Password

Language: English ▾

**CRITICAL** Nessus Plugin ID 61708

Information

Dependencies

Dependents

Changelog

### Synopsis

A VNC server running on the remote host is secured with a weak 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.

### Plugin Details

**Severity:** Critical

**ID:** 61708

**File Name:** vnc\_password\_password.nasl

**Version:** Revision: 1.2

**Type:** remote

**Family:** [Gain a shell remotely](#)

**Published:** 8/29/2012

**Updated:** 9/24/2015

**Supported Sensors:** Nessus

La password VNC è memorizzata nel file `~/.vnc/passwd`. La password viene memorizzata in questa posizione quando il server VNC viene avviato per la prima volta.

Per aggiornare o modificare la tua password VNC dovresti usare il comando `vncpasswd`.

`vncpasswd` ti chiederà due volte di inserire la nuova password:

```
$ vncpasswd
```

Password:

Verify:

Il comando `vncpasswd` accetta anche l'immissione di una password da STDIN che consente anche di archiviare il file della password in una posizione diversa.

L'esempio seguente modificherà la password VNC in `MYVNCPASSWORD` e la memorizzerà in `~/.secret/vncpass` dato che esiste la directory `.secret`:

```
$ echo MYVNCPASSWORD | vncpasswd -f > ~/.secret/passvnc
```

## Bind Shell Backdoor Detection

# Bind Shell Backdoor Detection

Language: English ▾

**CRITICAL**

Nessus Plugin ID 51988

Information

Dependencies

Dependents

Changelog

## Synopsis

The remote host may have been compromised.

## Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

## Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

## Plugin Details

**Severity:** Critical

**ID:** 51988

**File Name:**

wild\_shell\_backdoor.nasl

**Version:** 1.10

**Type:** remote

**Family:** Backdoors

**Published:** 2/15/2011

**Updated:** 4/11/2022

**Configuration:** Enable thorough checks

**Supported Sensors:**

Nessus

In questa situazione basta chiudere porta firewall 1524.

Abilitando la funzione del firewall: Block, non facendo capire all' attaccante che la porta è chiusa.

In questo modo si risolve il problema.



Filter Search Vulnerabilities 62 Vulnerabilities							
<input type="checkbox"/> Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1		
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1		
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1		
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2		
<input type="checkbox"/> MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4		
<input type="checkbox"/> CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3		
<input type="checkbox"/> HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1		
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1		
<input type="checkbox"/> MIXED	...	...	SSL (Multiple Issues)	General	28		
<input type="checkbox"/> MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5		
<input type="checkbox"/> MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2		
<input type="checkbox"/> MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1		