TRACCIA

Sev	Score	Name
CRITICAL	10.0 *	NFS Exported Share Information Disclosure
CRITICAL	10.0 *	rexecd Service Detection
CRITICAL	10.0	Unix Operating System Unsupported Version Detection
CRITICAL	10.0 *	VNC Server 'password' Password
CRITICAL	9.8	Bind Shell Backdoor Detection

Risolviamo solamente I problemi evidenziati in giallo.

NFS Exported Share Information Disclosure

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:

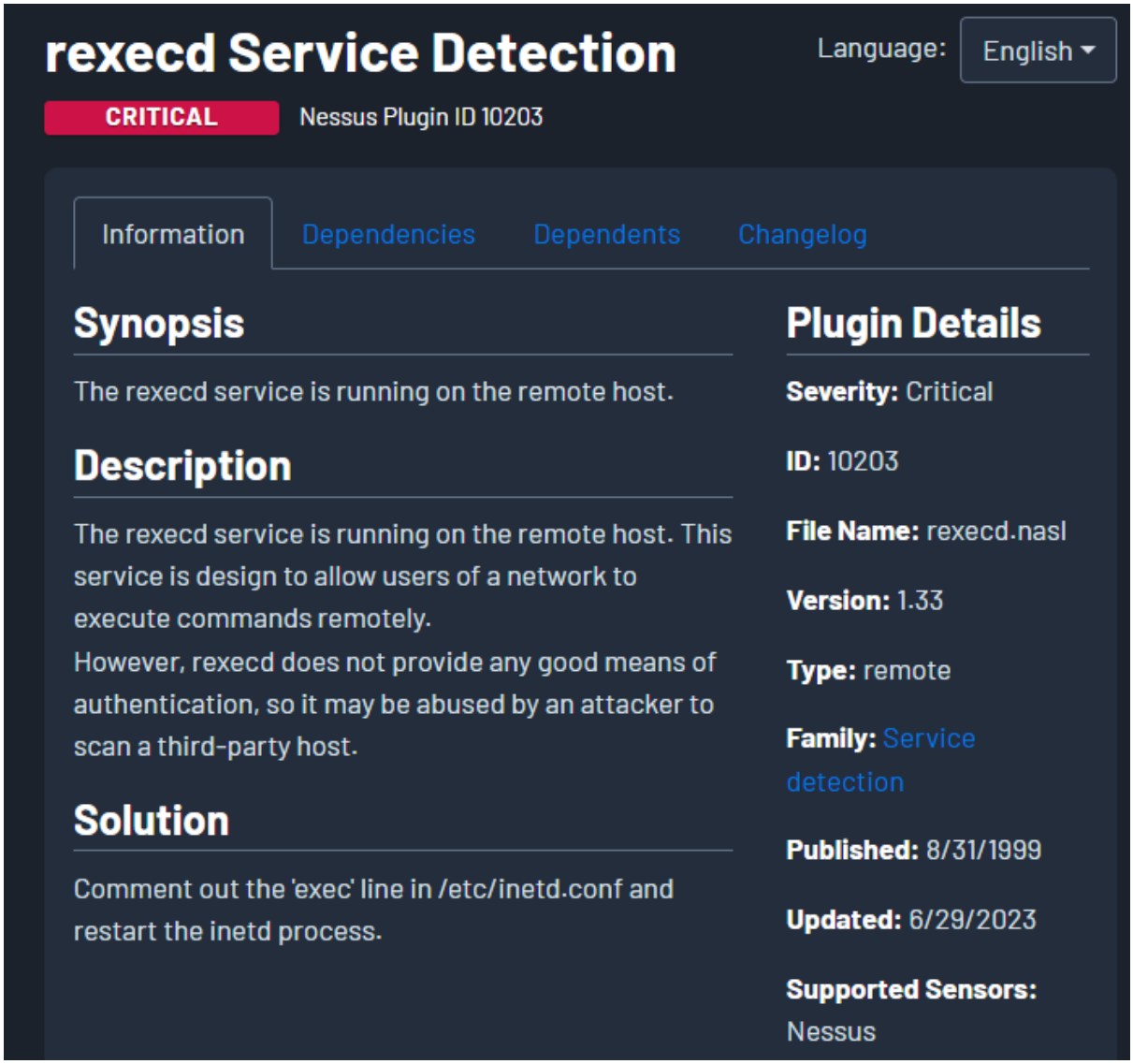
Gain Access

Soluzione

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

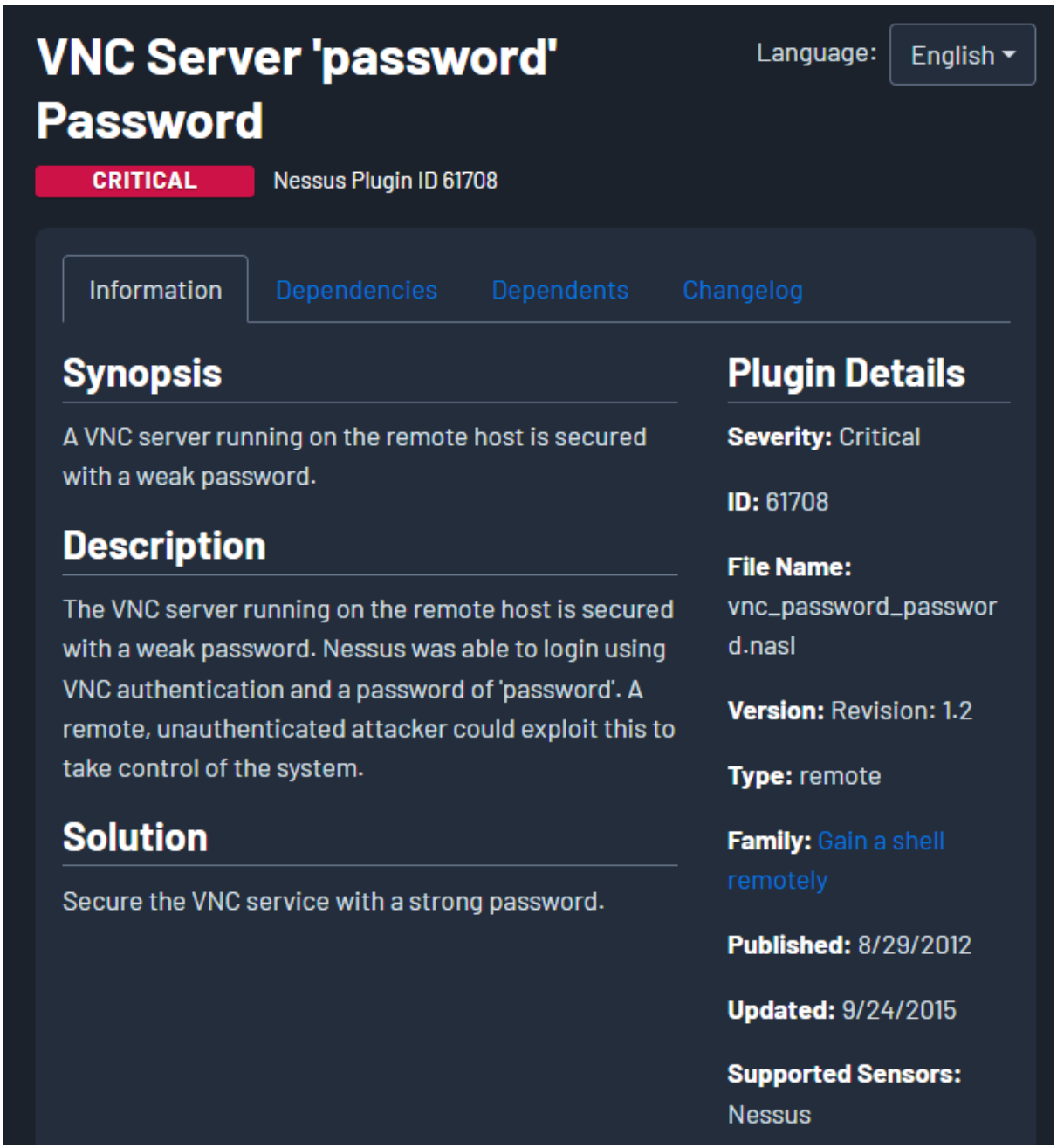
After installing the patch, run fsirand on your entire file system. The new fsirand program makes it difficult for a remote system user to guess NFS filehandles, preventing the user from conducting unauthorized mounts and accessing your NFS file systems.

rexecd Service Detection



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



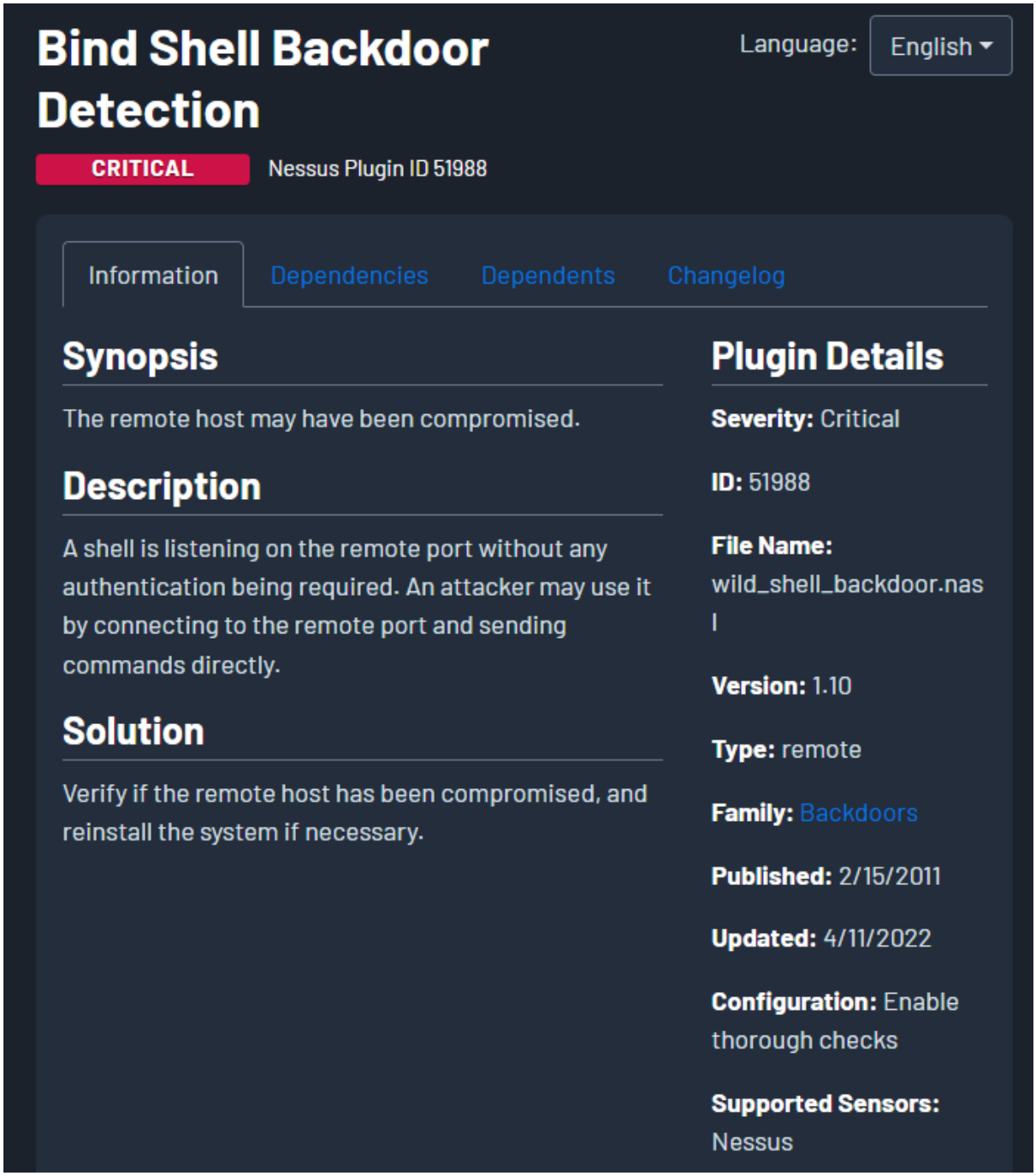
La password VNC è memorizzata nel file ~/.vnc/passwd. La password viene memorizzata in questa posizione quando il server VNC viene avviato per la prima volta.

Per aggiornare o modificare la tua password VNC dovresti usare il comando vncpasswd.
vncpasswd ti chiederà due volte di inserire la nuova password:

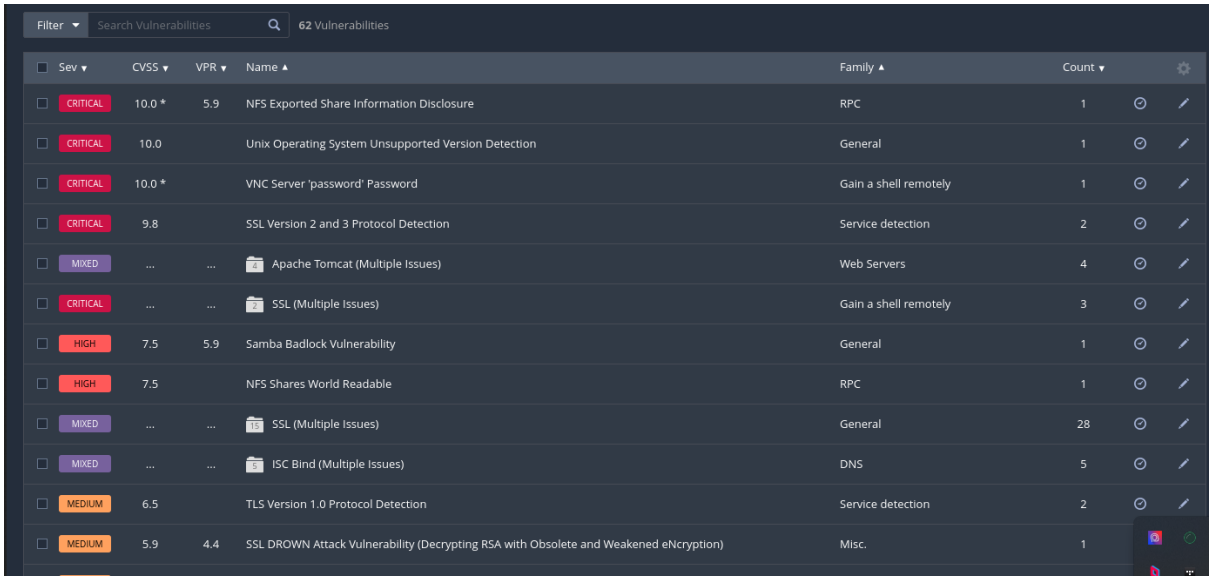
$ vncpasswd
Password:
Verify:

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



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
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 SSL Version 2 and 3 Protocol Detection Service detection 2
MIXED ... ... Apache Tomcat (Multiple Issues) Web Servers 4
CRITICAL ... ... SSL (Multiple Issues) Gain a shell remotely 3
HIGH 7.5 5.9 Samba Badlock Vulnerability General 1
HIGH 7.5 NFS Shares World Readable RPC 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 5.9 4.4 SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) Misc. 1