

# REPORT TECNICO DELLE VULNERABILITA'

192.168.49.101



#### Scan Information

Start time: Thu Feb 23 02:22:45 2023  
End time: Thu Feb 23 02:34:04 2023

#### Host Information

Netbios Name: METASPLOITABLE  
IP: 192.168.49.101  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

## Considerazioni generali

Dai risultati delle nostre operazioni ci risultano svariate vulnerabilità, molte anche particolarmente gravi, che comportano quindi seri rischi per i sistemi aziendali.

Alcune di esse permettono a potenziali malintenzionati di assumere il completo controllo dei sistemi aziendali, quindi avendo accesso a file e cartelle riservate, oppure il totale spegnimento ed eliminazione di qualsiasi servizio presente sul server analizzato.

## Misure da adottare

Di seguito elencheremo una serie di misure da effettuare per risolvere i problemi di sicurezza presenti al interno dei sistemi aziendali da noi analizzati.

Partendo dalle vulnerabilità gravi:

### 20007 (2) - SSL Version 2 and 3 Protocol Detection

#### In breve

Il servizio remoto critta il traffico usando un protocollo che presenta note debolezze

#### Descrizione

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affetti da diversi difetti crittografici, tra cui:

- Uno schema di padding insicuro con cifrari CBC.

- Schemi di rinegoziazione e ripresa delle sessioni insicuri.

Un utente malintenzionato può sfruttare questi difetti per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i client.

Sebbene SSL / TLS abbia un mezzo sicuro per scegliere la versione più supportata del protocollo (quindi che queste versioni verranno utilizzate solo se il client o il server non supportano nulla di meglio), molti browser web implementano questa operazione in modo non sicuro che consente a un utente malintenzionato di eseguire il downgrade di una connessione, ad esempio in POODLE.

Pertanto, si consiglia di disabilitare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. Alla data di applicazione trovata in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di PCI SSC di "forte" crittografia».

## Soluzione proposta

Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0.

Usare invece TSL 1.2 (Con suite di cifratura approvata) o superiore.

**32321 (2) - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**

## In breve

Il certificato remoto SSL usa una chiave debole.

## Descrizione

Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto al fatto che un packager Debian rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the middle.

## Soluzione proposta

Considerare tutto il materiale crittografato come inaffidabile. In particolare qualsiasi chiave di SSH, SSL e OpenVPN, andrebbe rigenerata.

## **11356 (1) - NFS Exported Share Information Disclosure**

### **In breve**

E' possibile accedere da remoto alle cartelle NFS del server.

### **Descrizione**

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione.

Un attaccante potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

### **Soluzione proposta**

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

## **33850 (1) - Unix Operating System Unsupported Version Detection**

### **In breve**

Il sistema operativo non è più supportato.

### **Descrizione**

Secondo il suo numero di versione auto-riportato, il sistema operativo Unix in esecuzione sull'host remoto è non più supportato.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Quindi è probabile che contenga vulnerabilità di sicurezza.

### **Soluzione proposta**

Aggiornare il sistema a una versione di Unix supportata

## **51988 (1) - Bind Shell Backdoor Detection**

### **In breve**

E' presente una backdoor sul sistema.

### **Descrizione**

Una shell è in ascolto sulla porta remota 1524 senza che sia richiesta alcuna autenticazione.

Un utente malintenzionato può usarlo per collegarsi alla porta remota e inviare direttamente i comandi.

### **Soluzione proposta**

Controllare che il sistema non sia stato compromesso, e se necessario reinstallare il sistema.

## **61708 (1) - VNC Server 'password' Password**

### **In breve**

Un servizio VNC che gira sul server remoto ha una password debole.

### **Descrizione**

Il server VNC in esecuzione sull'host remoto è protetto da una password debole.

Il nostro esperto è riuscito ad accedere utilizzando l'autenticazione VNC e una password: 'password'.

Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questo metodo per prendere il controllo del sistema.

### **Soluzione proposta**

Cambiare password, utilizzando una password solida.

## 134862 (1) - Apache Tomcat AJP Connector Request Injection (Ghostcat)

### In breve

C'è un connettore AJP vulnerabile in ascolto sull'host remoto.

### Descrizione

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP.

Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file dell'applicazione Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

### Soluzione proposta

Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

Vulnerabilità a rischio alto:

## 42873 (2) - SSL Medium Strength Cipher Suites Supported (SWEET32)

## 26928 (1) - SSL Weak Cipher Suites Supported

## 31705 (1) - SSL Anonymous Cipher Suites Supported

## 81606 (1) - SSL/TLS EXPORT\_RSA <= 512-bit Cipher Suites Supported (FREAK)

## 83738 (1) - SSL/TLS EXPORT\_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

### In breve

Il servizio remoto supporta una crittografia SSL non abbastanza forte e anonima.

### Descrizione

L'host remoto supporta l'uso di crittografie SSL che offrono una crittografia di livello medio.

E' catalogata come forza media come qualsiasi crittografia che utilizzi lunghezze di chiave di almeno 64 bit e inferiori a 112 bit, oppure che utilizza la suite di crittografia 3DES.

Si noti che è notevolmente più semplice aggirare la crittografia di media potenza se l'attaccante si trova sulla stessa rete fisica.

L'host remoto supporta le suite di cifratura EXPORT\_RSA con chiavi inferiori o uguali a 512 bit. Un utente malintenzionato può fattorizzare un modulo RSA a 512 bit in un breve lasso di tempo.

Un utente malintenzionato man-in-the-middle potrebbe essere in grado di eseguire il downgrade della sessione per utilizzare le suite di crittografia EXPORT\_RSA (ad esempio CVE-2015-0204). Pertanto, si consiglia di rimuovere il supporto per le suite di cifratura deboli.

## Soluzione proposta

Riconfigurare l'applicazione per fare in modo che eviti di usare questo tipo di crittografia.

Riconfigurare il servizio per rimuovere il supporto per le suite di cifratura EXPORT\_RSA.

Riconfigurare il servizio per rimuovere il supporto per le suite di cifratura EXPORT\_DHE.

### 10205 (1) - rlogin Service Detection

### 10245 (1) - rsh Service Detection

## In breve

Il servizio rlogin e rsh sono attivi sull'host.

## Descrizione

Il servizio rlogin e rsh sono in esecuzione sull'host remoto.

Questi servizi sono vulnerabili poiché i dati vengono scambiati tra il client e il server in chiaro. Un utente malintenzionato con un man-in-the-middle può sfruttarlo per sniffare accessi e password.

Inoltre, potrebbe consentire accessi scarsamente autenticati senza password. Se l'host è vulnerabile all'ipotesi del numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (incluso il dirottamento ARP su una rete locale) allora potrebbe essere possibile bypassare l'autenticazione.

Infine, rlogin e rsh sono un modo semplice per trasformare l'accesso in scrittura ai file in accessi completi tramite i file .rhosts o rhosts.equiv.

## Soluzione proposta

Commentare la riga 'login' e 'rsh' in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilitare questo servizio e utilizzare invece SSH.

## **42256 (1) - NFS Shares World Readable**

### **In breve**

Il server remoto NFS esporta cartelle leggibili da tutti.

### **Descrizione**

Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP, o intervallo IP).

### **Soluzione proposta**

Impostare delle restrizioni adeguate alle cartelle NFS.

## **90509 (1) - Samba Badlock Vulnerability**

### **In breve**

Un server SMB in esecuzione sull'host remoto è interessato dalla vulnerabilità Badlock.

### **Descrizione**

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD ) a causa di una negoziazione errata del livello di autenticazione sui canali RPC (Remote Procedure Call).

Un attaccante man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati sensibili sulla sicurezza nel database di Active Directory (AD) o la disabilitazione di servizi critici.

### **Soluzione proposta**

Aggiornare Samba alla versione 4.2.11 / 4.3.8 / 4.4.2 o successiva.

**136769 (1) - ISC BIND Service Downgrade / Reflected DoS**

**136808 (1) - ISC BIND Denial of Service**

**139915 (1) - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS**

## In breve

Il server dei nomi remoto è interessato da vulnerabilità di downgrade del servizio/DoS riflesse.

Inoltre il server dei nomi remoto è interessato da una vulnerabilità di errore di asserzione.

Il server dei nomi remoto è affetto da una vulnerabilità Denial of Service.

## Descrizione

Secondo la sua versione auto-segnalata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è interessata dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse. Ciò è dovuto al fatto che BIND DNS non limita sufficientemente il numero di recuperi che possono essere eseguiti durante l'elaborazione di una risposta di riferimento.

Un utente malintenzionato remoto non autenticato può sfruttarlo per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione.

Esiste una vulnerabilità Denial of Service (DoS) nelle versioni ISC BIND 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 e precedenti. Un utente malintenzionato remoto non autenticato può sfruttare questo problema, tramite un messaggio appositamente predisposto, per impedire al servizio di rispondere.

In base al numero di versione auto-riportato, l'installazione di ISC BIND in esecuzione sul server dei nomi remoto è la versione 9.x precedente alla 9.11.22, 9.12.x precedente alla 9.16.6 o 9.17.x precedente alla 9.17.4. Pertanto, è affetto da una vulnerabilità di negazione del servizio (DoS) a causa di un errore di asserzione durante il tentativo di verificare una risposta troncata a una richiesta firmata da TSIG. Un utente malintenzionato remoto autenticato può sfruttare questo problema inviando una risposta troncata a una richiesta firmata TSIG per attivare un errore di asserzione, causando la chiusura del server.

Si noti che l'analisi non ha testato questo problema, ma si è invece basata solo sul numero di versione auto-riportato dell'applicazione.

## Soluzione proposta

Aggiornare la versione di ISC BIND alla versione consigliata dal venditore.

Aggiorna alla versione con patch più strettamente correlata alla attuale versione di BIND.

Aggiorna a BIND 9.11.22, 9.16.6, 9.17.4 o successivo.

Di seguito l'elenco delle vulnerabilità di rischio moderato, alcune di esse sono risolte a cascata da alcune delle risoluzioni sopra esposte se si cambia servizio utilizzato.

**15901 (2) - SSL Certificate Expiry**

**45411 (2) - SSL Certificate with Wrong Hostname**

**51192 (2) - SSL Certificate Cannot Be Trusted**

**57582 (2) - SSL Self-Signed Certificate**

## In breve

Ci sono una serie di problemi con i certificati del servizio SSL.

## Descrizione

Il certificato associato al servizio SSL è scaduto.

L'attributo 'commonName' (CN) del certificato SSL presentato per questo servizio è per una macchina diversa.

Il certificato X.509 del server non può essere attendibile. Questa situazione può verificarsi in tre modi diversi, in cui la catena della fiducia può essere spezzata, come indicato di seguito:

- Innanzitutto, la parte superiore della catena di certificati inviata dal server potrebbe non discendere da un'autorità di certificazione pubblica nota. Ciò può verificarsi quando la parte superiore della catena è un'autofirmata non riconosciuta certificato o quando mancano certificati intermedi che collegherebbero la parte superiore della catena di certificati a un'autorità di certificazione pubblica nota.
- In secondo luogo, la catena di certificati potrebbe contenere un certificato non valido al momento della scansione. Ciò può verificarsi quando la scansione avviene prima di una delle date "notBefore" del certificato o dopo una delle date "notAfter" del certificato.
- In terzo luogo, la catena di certificati potrebbe contenere una firma che non corrispondeva alle informazioni del certificato o che non poteva essere verificata. Le firme errate possono essere corrette facendo firmare nuovamente il certificato con la firma errata dall'emittente. Le firme che non è stato possibile verificare sono il risultato dell'utilizzo da parte dell'emittente del certificato di un algoritmo di firma che non è riconosciuto.

Se l'host remoto è un host pubblico in produzione, qualsiasi interruzione nella catena rende più difficile per gli utenti verificare l'autenticità e l'identità del server web. Ciò potrebbe semplificare l'esecuzione di attacchi man-in-the-middle contro l'host remoto.

La catena di certificati X.509 per questo servizio non è firmata da un'autorità di certificazione riconosciuta. Se l'host remoto è un host pubblico in produzione, ciò annulla l'uso di SSL poiché chiunque potrebbe stabilire un attacco man-in-the-middle contro l'host remoto.

Tieni presente che questo plug-in non verifica la presenza di catene di certificati che terminano con un certificato non autofirmato, ma firmato da un'autorità di certificazione non riconosciuta

## Soluzione proposta

Acquistare o generare un nuovo certificato SSL per sostituire quello esistente.

### 65821 (2) - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

## In breve

Il servizio remoto supporta l'uso della cifratura RC4.

## Descrizione

L'host remoto supporta l'uso di RC4 in una o più suite di cifratura.

Il cifrario RC4 è imperfetto nella sua generazione di un flusso di byte pseudo-casuale in modo che un'ampia varietà di piccoli pregiudizi venga introdotta nel flusso, diminuendo la sua casualità.

Se il testo in chiaro viene crittografato ripetutamente (ad esempio, i cookie HTTP) e un utente malintenzionato è in grado di ottenere molti (cioè decine di milioni) testi cifrati, l'attaccante potrebbe essere in grado di derivare il testo in chiaro.

## Soluzione proposta

Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di crittografie RC4.

Prendere in considerazione l'utilizzo di TLS 1.2 con le suite AES-GCM soggette al supporto del browser e del server Web.

## **78479 (2) - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)**

## **89058 (1) - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)**

### **In breve**

È possibile ottenere informazioni riservate dall'host remoto con servizi abilitati per SSL/TLS.

### **Descrizione**

L'host remoto è affetto da una vulnerabilità di divulgazione di informazioni man-in-the-middle (MitM) nota come POODLE. La vulnerabilità è dovuta al modo in cui SSL 3.0 gestisce i byte di riempimento durante la decrittografia dei messaggi crittografati utilizzando cifrari a blocchi in modalità Cipher Block Chaining (CBC).

Gli aggressori MitM possono decrittografare un byte selezionato di un testo cifrato in appena 256 tentativi se sono in grado di forzare un'applicazione vittima a inviare ripetutamente gli stessi dati su connessioni SSL 3.0 appena create.

Finché un client e un servizio supportano entrambi SSLv3, è possibile eseguire il "rollback" di una connessione a SSLv3, anche se TLSv1 o più recente è supportato dal client e dal servizio.

Il meccanismo TLS Fallback SCSV impedisce gli attacchi di "rollback della versione" senza influire sui client legacy; tuttavia, può proteggere le connessioni solo quando il client e il servizio supportano il meccanismo. I siti che non possono disabilitare SSLv3 immediatamente dovrebbero abilitare questo meccanismo.

Questa è una vulnerabilità nella specifica SSLv3, non in una particolare implementazione SSL. La disabilitazione di SSLv3 è l'unico modo per mitigare completamente la vulnerabilità.

L'host remoto supporta SSLv2 e pertanto può essere affetto da una vulnerabilità che consente un attacco racle di riempimento Bleichenbacher incrociato noto come DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Questa vulnerabilità esiste a causa di un difetto nell'implementazione di Secure Sockets Layer Version 2 (SSLv2) e consente la decrittografia del traffico TLS acquisito. Un utente malintenzionato man-in-the-middle può sfruttarlo per decrittografare la connessione TLS utilizzando traffico acquisito in precedenza e crittografia debole insieme a una serie di connessioni appositamente predisposte a un server SSLv2 che utilizza la stessa chiave privata.

### **Soluzione proposta**

Disabilitare SSLv3.

I servizi che devono supportare SSLv3 devono abilitare il meccanismo SCSV di fallback TLS finché SSLv3 non può essere disabilitato.

Disabilita SSLv2 ed esporta suite di crittografia di livello di crittografia. Assicurati che le chiavi private non vengano utilizzate da nessuna parte con il software server che supporta le connessioni SSLv2.

## 104743 (2) - TLS Version 1.0 Protocol Detection

### In breve

Il servizio remoto crittografa il traffico utilizzando una versione precedente di TLS.

### Descrizione

Il servizio remoto accetta connessioni crittografate tramite TLS 1.0. TLS 1.0 presenta una serie di difetti di progettazione crittografica. Le moderne implementazioni di TLS 1.0 mitigano questi problemi, ma le versioni più recenti di TLS come 1.2 e 1.3 sono progettate contro questi difetti e dovrebbero essere utilizzate quando possibile.

A partire dal 31 marzo 2020, gli endpoint non abilitati per TLS 1.2 e versioni successive non funzioneranno più correttamente con i principali browser Web e i principali fornitori.

PCI DSS v3.2 richiede che TLS 1.0 sia disabilitato completamente entro il 30 giugno 2018, ad eccezione dei terminali POS POI (e dei punti di terminazione SSL/TLS a cui si connettono) che possono essere verificati come non soggetti a exploit noti.

### Soluzione proposta

Abilitare il supporto per TLS 1.2 e 1.3 e disabilitare il supporto per TLS 1.0.

## 12085 (1) - Apache Tomcat Default Files

### In breve

Il server Web remoto contiene file predefiniti.

### Descrizione

La pagina di errore predefinita, la pagina indice predefinita, i JSP di esempio e/o servlet di esempio sono installati sul server Apache Tomcat remoto. Questi file dovrebbero essere rimossi in quanto potrebbero aiutare un utente malintenzionato a scoprire informazioni sull'installazione remota di Tomcat o sull'host stesso.

### Soluzione proposta

Elimina la pagina indice predefinita e rimuovi JSP e servlet di esempio. Segui le istruzioni di Tomcat o OWASP per sostituire o modificare la pagina di errore predefinita.

## 42263 (1) - Unencrypted Telnet Server

### In breve

Il server Telnet remoto trasmette il traffico in chiaro.

### Descrizione

L'host remoto esegue un server Telnet su un canale non crittografato.

L'utilizzo di Telnet su un canale non crittografato non è consigliato poiché accessi, password e comandi vengono trasferiti in chiaro. Ciò consente a un utente malintenzionato remoto, man-in-the-middle, di intercettare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e modificare il traffico scambiato tra un client e server.

SSH è preferibile a Telnet poiché protegge le credenziali dall'intercettazione e può eseguire il tunneling di flussi di dati aggiuntivi come una sessione X11.

### Soluzione proposta

Disabilitare il servizio Telnet e usare invece SSH.

## 52611 (1) - SMTP Service STARTTLS Plaintext Command Injection

### In breve

Il servizio di posta remota consente l'inserimento di comandi in chiaro durante la negoziazione di un canale di comunicazione crittografato.

### Descrizione

Il servizio SMTP remoto contiene un difetto software nella sua implementazione STARTTLS che potrebbe consentire a un utente malintenzionato remoto e non autenticato di inserire comandi durante la fase del protocollo di testo in chiaro che verranno eseguiti durante la fase del protocollo di testo cifrato.

Uno sfruttamento riuscito potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o le credenziali SASL (Simple Authentication and Security Layer) associate.

### Soluzione proposta

Contattare il fornitore per vedere se è disponibile un aggiornamento.

## **57608 (1) - SMB Signing not required**

### **In breve**

La firma non è richiesta sul server SMB remoto.

### **Descrizione**

La firma non è richiesta sul server SMB remoto. Un utente malintenzionato remoto non autenticato può sfruttarlo per condurre attacchi man-in-the-middle contro il server SMB.

### **Soluzione proposta**

Imporre la firma dei messaggi nella configurazione dell'host. Su Windows, questo si trova nell'impostazione del criterio "Server di rete Microsoft: aggiungi firma digitale alle comunicazioni (sempre)". Su Samba, l'impostazione si chiama "firma del server".

## **90317 (1) - SSH Weak Algorithms Supported**

## **70658 (1) - SSH Server CBC Mode Ciphers Enabled**

## **71049 (1) - SSH Weak MAC Algorithms Enabled**

## **153953 (1) - SSH Weak Key Exchange Algorithms Enabled**

### **In breve**

Il server SSH remoto è configurato per consentire algoritmi di crittografia deboli o nessun algoritmo.

Il server SSH è configurato per utilizzare Cipher Block Chaining.

Il server SSH remoto è configurato per consentire algoritmi di scambio di chiavi deboli.

### **Descrizione**

E' stato rilevato che il server SSH remoto è configurato per utilizzare la cifratura a flusso Arcfour o nessuna cifratura. RFC 4253 sconsiglia l'utilizzo di Arcfour a causa di un problema con chiavi deboli.

Il server SSH è configurato per supportare la crittografia Cipher Block Chaining (CBC). Ciò può consentire a un utente malintenzionato di recuperare il messaggio in chiaro dal testo cifrato.

## **Soluzione proposta**

Contattare il fornitore o consultare la documentazione del prodotto per rimuovere le cifrature e gli algoritmi deboli.

### **10407 (1) - X Server Detection**

#### **In breve**

Un server X11 è in ascolto sull'host remoto.

#### **Descrizione**

L'host remoto esegue un server X11. X11 è un protocollo client-server che può essere utilizzato per visualizzare applicazioni grafiche in esecuzione su un determinato host su un client remoto.

Poiché il traffico X11 non è cifrato, è possibile che un utente malintenzionato intercetti la connessione.

#### **Soluzione proposta**

Limita l'accesso a questa porta. Se la funzionalità client/server X11 non viene utilizzata, disabilitare completamente il supporto TCP in X11 (-nolisten tcp).

Di seguito solo uno schema con quelle che sono considerate di livello info, cioè non una vera vulnerabilità, ma un modo di ottenere informazioni a riguardo del sistema:

|      |     |                        |   |
|------|-----|------------------------|---|
| INFO | N/A | <a href="#">10114</a>  | ICMP Timestamp Request Remote Date Disclosure                               |
| INFO | N/A | <a href="#">10223</a>  | RPC portmapper Service Detection  |
| INFO | N/A | <a href="#">21186</a>  | AJP Connector Detection   |
| INFO | N/A | <a href="#">39446</a>  | Apache Tomcat Detection   |
| INFO | N/A | <a href="#">39519</a>  | Backported Security Patch Detection (FTP)                                   |
|      |     |                        |   |
| INFO | N/A | <a href="#">39520</a>  | Backported Security Patch Detection (SSH)                                   |
| INFO | N/A | <a href="#">45590</a>  | Common Platform Enumeration (CPE)   |
| INFO | N/A | <a href="#">10028</a>  | DNS Server BIND version Directive Remote Version Detection                  |
| INFO | N/A | <a href="#">11002</a>  | DNS Server Detection  |
| INFO | N/A | <a href="#">72779</a>  | DNS Server Version Detection  |
| INFO | N/A | <a href="#">35371</a>  | DNS Server hostname.bind Map Hostname Disclosure                            |
| INFO | N/A | <a href="#">54615</a>  | Device Type   |
| INFO | N/A | <a href="#">10092</a>  | FTP Server Detection  |
| INFO | N/A | <a href="#">10107</a>  | HTTP Server Type and Version  |
| INFO | N/A | <a href="#">24260</a>  | HyperText Transfer Protocol (HTTP) Information                              |
| INFO | N/A | <a href="#">10397</a>  | Microsoft Windows SMB LanMan Pipe Server Listing Disclosure                 |
| INFO | N/A | <a href="#">10785</a>  | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure |
| INFO | N/A | <a href="#">11011</a>  | Microsoft Windows SMB Service Detection                                     |
| INFO | N/A | <a href="#">100871</a> | Microsoft Windows SMB Versions Supported (remote check)                     |
| INFO | N/A | <a href="#">106716</a> | Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)           |
| INFO | N/A | <a href="#">10437</a>  | NFS Share Export List   |
| INFO | N/A | <a href="#">11219</a>  | Nessus SYN scanner  |
| INFO | N/A | <a href="#">19506</a>  | Nessus Scan Information   |
| INFO | N/A | <a href="#">11936</a>  | OS Identification   |

|      |     |        |  |
|------|-----|--------|--|
| INFO | N/A | 117886 | OS Security Patch Assessment Not Available                                   |
| INFO | N/A | 10919  | Open Port Re-check   |
| INFO | N/A | 50845  | OpenSSL Detection  |
| INFO | N/A | 66334  | Patch Report   |
| INFO | N/A | 118224 | PostgreSQL STARTTLS Support  |
| INFO | N/A | 26024  | PostgreSQL Server Detection  |
|      |     |        |  |
| INFO | N/A | 22227  | RMI Registry Detection   |
| INFO | N/A | 11111  | RPC Services Enumeration   |
| INFO | N/A | 53335  | RPC portmapper (TCP)   |
| INFO | N/A | 10263  | SMTP Server Detection  |
| INFO | N/A | 42088  | SMTP Service STARTTLS Command Support  |
| INFO | N/A | 70657  | SSH Algorithms and Languages Supported                                       |
| INFO | N/A | 149334 | SSH Password Authentication Accepted   |
| INFO | N/A | 10881  | SSH Protocol Versions Supported  |
| INFO | N/A | 153588 | SSH SHA-1 HMAC Algorithms Enabled  |
| INFO | N/A | 10267  | SSH Server Type and Version Information                                      |
| INFO | N/A | 56984  | SSL / TLS Versions Supported   |
| INFO | N/A | 45410  | SSL Certificate 'commonName' Mismatch  |
| INFO | N/A | 10863  | SSL Certificate Information  |
| INFO | N/A | 70544  | SSL Cipher Block Chaining Cipher Suites Supported                            |
| INFO | N/A | 21643  | SSL Cipher Suites Supported  |
| INFO | N/A | 57041  | SSL Perfect Forward Secrecy Cipher Suites Supported                          |
| INFO | N/A | 51891  | SSL Session Resume Supported   |
| INFO | N/A | 156899 | SSL/TLS Recommended Cipher Suites  |
| INFO | N/A | 25240  | Samba Server Detection   |
| INFO | N/A | 104887 | Samba Version  |
| INFO | N/A | 96982  | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) |

|      |     |        |   |
|------|-----|--------|---|
| INFO | N/A | 22964  | Service Detection   |
| INFO | N/A | 17975  | Service Detection (GET request)   |
| INFO | N/A | 25220  | TCP/IP Timestamps Supported   |
| INFO | N/A | 11819  | TFTP Daemon Detection   |
|      |     |        |   |
| INFO | N/A | 110723 | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | 10281  | Telnet Server Detection   |
| INFO | N/A | 10287  | Traceroute Information  |
| INFO | N/A | 11154  | Unknown Service Detection: Banner Retrieval                                   |
| INFO | N/A | 19288  | VNC Server Security Type Detection  |
| INFO | N/A | 65792  | VNC Server Unencrypted Communication Detection                                |
| INFO | N/A | 10342  | VNC Software Detection  |
| INFO | N/A | 135860 | WMI Not Available   |
| INFO | N/A | 20108  | Web Server / Application favicon.ico Vendor Fingerprinting                    |
| INFO | N/A | 11422  | Web Server Unconfigured - Default Install Page Present                        |
| INFO | N/A | 10150  | Windows NetBIOS / SMB Remote Host Information Disclosure                      |
| INFO | N/A | 52703  | vsftpd Detection  |