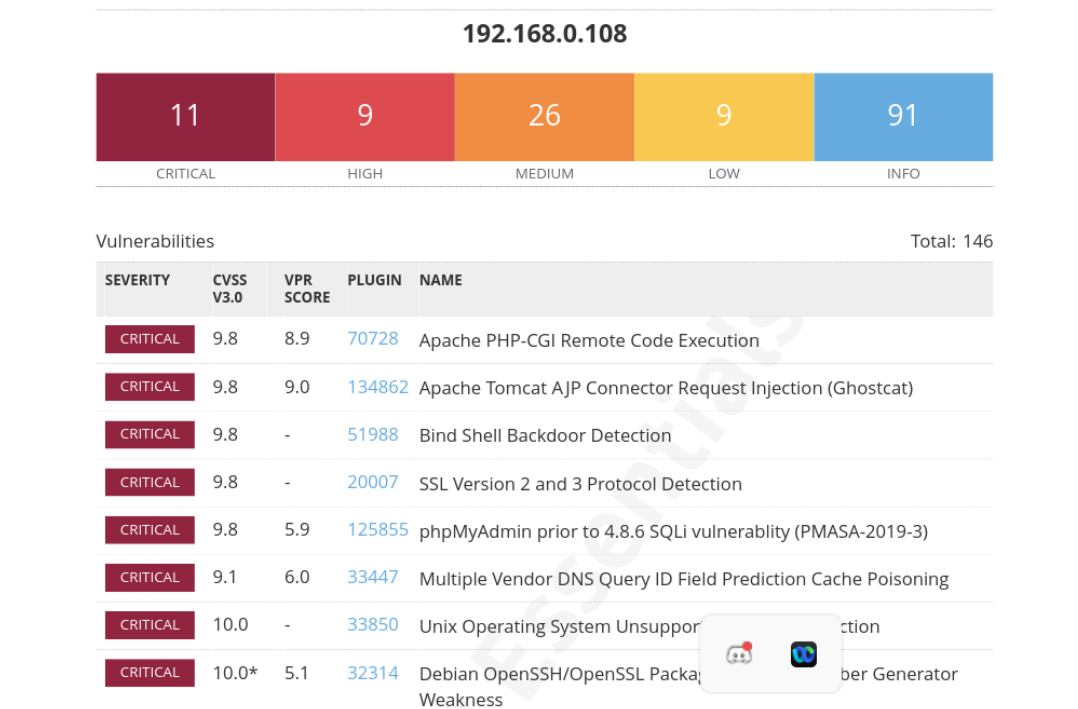


## REPORT VULNERABILITA' TROVATE SU METASPLOITABLE CON SCANSIONE SU NESSUS



Dopo aver effettuato la scansione, sono risultate 11 vulnerabilità critiche, 9 alte, 26 medie, 9 basse e 91 info.

Analizziamo nel dettaglio 3 vulnerabilità critiche e spieghiamo come risolverle.

Vulnerability Assessment su Metasploitable / Plugin #11356

[← Back to Vulnerabilities](#)

Hosts 1 | **Vulnerabilities 88** | Remediations 4 | History 2

**CRITICAL** NFS Exported Share Information Disclosure

**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.

**Output**

```
The following NFS shares could be mounted :  
  
+ /  
+ Contents of / :  
- .  
- ..  
- bbbbbbRD#####11N  
- bin  
- boot  
more...
```

To see debug logs, please visit individual host

| Port                 | Hosts         |
|----------------------|---------------|
| 2049 / udp / rpc-nfs | 192.168.0.108 |

**1 VULNERABILITA':** Questa vulnerabilità è classificata come una "NFS Exported Share Information Disclosure", il che significa che almeno una delle condivisioni NFS esportate dal server remoto può essere montata dall'host di scansione. Ciò potrebbe consentire a un attaccante di leggere (e forse scrivere) file sull'host remoto.

La soluzione raccomandata è configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Per risolvere questa vulnerabilità, è necessario rivedere e riconfigurare le impostazioni di NFS sull'host remoto. Assicurarsi di impostare correttamente le autorizzazioni in modo che solo gli host autorizzati possano accedere e montare le condivisioni NFS. Si può fare ciò modificando il file di configurazione NFS (solitamente /etc/exports su sistemi Linux) per specificare quali host o reti sono autorizzati ad accedere alle condivisioni e quali diritti hanno.

Una volta apportate le modifiche necessarie alla configurazione di NFS, riavviare il servizio NFS sull'host remoto per applicare le modifiche.

Inoltre, bisogna assicurarsi di monitorare regolarmente la configurazione NFS per garantire che non ci siano ulteriori esposizioni non desiderate e di effettuare aggiornamenti di sicurezza regolari per mitigare nuove vulnerabilità.

## 2 VULNERABILITA':

Vulnerability Assessment su Metasploitable / Plugin #33850

[← Back to Vulnerabilities](#)

Hosts1

Vulnerabilities88

Remediations4

History2

CRITICAL

Unix Operating System Unsupported Version Detection

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Output

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .

For more information, see : https://wiki.ubuntu.com/Releases
```

To see debug logs, please visit individual host

| Port ▲ | Hosts         |
|--------|---------------|
| N/A    | 192.168.0.108 |

Questa vulnerabilità indica che il sistema operativo Unix in esecuzione sull'host remoto ha raggiunto la fine del suo ciclo di supporto. Ciò significa che il fornitore non rilascerà ulteriori patch di sicurezza per questa

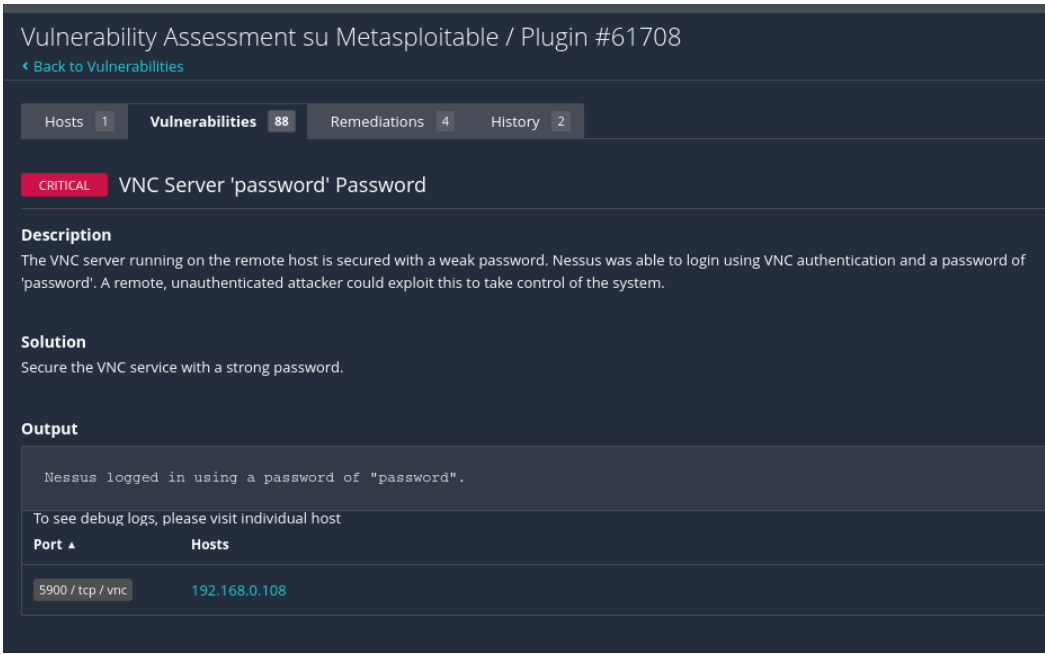
versione del sistema operativo, lasciandolo potenzialmente vulnerabile a minacce di sicurezza note e future.

La soluzione consigliata è quella di eseguire l'aggiornamento a una versione del sistema operativo Unix attualmente supportata. Questo garantirà che il sistema riceva regolarmente aggiornamenti di sicurezza per proteggere contro le vulnerabilità note e per mantenere un ambiente sicuro.

Per eseguire l'aggiornamento, è necessario seguire le procedure raccomandate dal fornitore del sistema operativo. Questo di solito coinvolge l'esecuzione di comandi specifici per aggiornare il sistema operativo e le sue applicazioni alla versione più recente supportata.

Assicurarsi di eseguire regolarmente gli aggiornamenti di sicurezza è fondamentale per mantenere un ambiente informatico sicuro e proteggere i dati sensibili da minacce di sicurezza.

### 3 VULNERABILITA':



The screenshot shows a Nessus vulnerability assessment interface. At the top, it says 'Vulnerability Assessment su Metasploitable / Plugin #61708'. Below this is a navigation bar with tabs: 'Hosts 1', 'Vulnerabilities 88', 'Remediations 4', and 'History 2'. The main content area displays a 'CRITICAL' vulnerability titled 'VNC Server 'password' Password'. The 'Description' states: '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.' The 'Solution' section advises: 'Secure the VNC service with a strong password.' The 'Output' section shows a log entry: 'Nessus logged in using a password of "password".' Below this, there is a table with headers 'Port' and 'Hosts'. The table contains one entry: '5900 / tcp / vnc' and '192.168.0.108'.

| Port             | Hosts         |
|------------------|---------------|
| 5900 / tcp / vnc | 192.168.0.108 |

Questa vulnerabilità evidenzia un problema di sicurezza comune con i server VNC: l'utilizzo di una password debole o predefinita. Se il server VNC è configurato con una password come "password" o altre password deboli, un potenziale attaccante potrebbe sfruttare questa vulnerabilità per ottenere accesso non autorizzato al sistema.

La soluzione raccomandata è quella di proteggere il servizio VNC con una password robusta e sicura. Una password sicura dovrebbe essere lunga, complessa e unica per ogni servizio. Evitare di utilizzare parole comuni, come "password", o sequenze facilmente indovinabili. È consigliabile utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali.

Per risolvere questa vulnerabilità, è necessario cambiare la password del server VNC e assicurarsi che sia configurata con una password robusta e sicura. Assicurarsi di seguire le migliori pratiche di sicurezza per la gestione delle password, come la regolare rotazione delle password e la memorizzazione sicura delle stesse.

Monitora regolarmente la configurazione del server VNC per garantire che non ci siano altre vulnerabilità di sicurezza e prendi le misure necessarie per mitigare eventuali rischi di sicurezza.