

La prima vulnerabilità

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 / :  
- .  
- .  
- bin  
- boot  
- mail  
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.1.10

consente a un utente non autorizzato di accedere alle condivisioni NFS di un host remoto. Infatti, tale utente potrebbe sfruttare questa vulnerabilità per accedere a file sensibili o dati riservati. Si potrebbe anche utilizzare la vulnerabilità per ottenere un accesso privilegiato all'host remoto.

Per risolvere questa vulnerabilità, è necessario configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le condivisioni NFS remote.

In alternativa, è possibile utilizzare un firewall per bloccare l'accesso alle condivisioni NFS da parte di host non autorizzati.

La seconda vulnerabilità

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	192.168.1.10

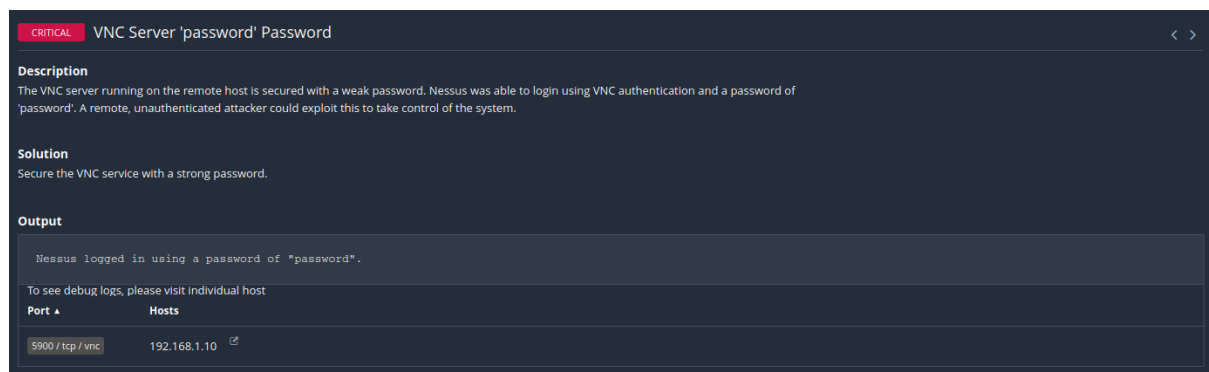
riguarda la versione non supportata del sistema operativo Unix. Ciò significa che il sistema operativo in esecuzione sull'host remoto non è più supportato dal fornitore. La mancanza di supporto implica che il

fornitore non rilascerà più patch di sicurezza per il prodotto. Di conseguenza, è probabile che il sistema operativo contenga vulnerabilità di sicurezza note.

Nello specifico, la vulnerabilità trovata rileva le versioni non supportate del sistema operativo Unix. In questo caso, il sistema operativo in esecuzione sull'host remoto è una versione di Debian 8.0, che è stata rilasciata nel 2015. Debian ha smesso di supportare questa versione nel 2017.

La soluzione a questa vulnerabilità è aggiornare il sistema operativo a una versione attualmente supportata. Nel caso di Debian, la versione attualmente supportata è Debian 11.

La terza vulnerabilità



identifica una password debole in un server VCN. Questa vulnerabilità consente ad un utente malintenzionato di accedere al server VCN senza alcuna autenticazione e controllarlo da remoto.

Il rapporto di Nessus indica che la password è “password”. Questa password è ovviamente debole.

La vulnerabilità è stata pubblicata per la prima volta nel 2012 ed è stata risolta nel 2015. Tuttavia, è possibile che alcuni server VCN non siano stati aggiornati alla versione più recente.

Per correggere questa vulnerabilità, è necessario aggiornare il server VCN alla versione più recente o modificare la password utilizzandone una più forte.

La quarta vulnerabilità

The screenshot displays the Tenable Nessus web interface. The top navigation bar includes links for Scans, Settings, and a user profile. The left sidebar contains navigation options for FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Tenable Scan). The main content area is titled 'root / Plugin #51988' and shows a 'Vulnerabilities' section with a 'CRITICAL' status for 'Bind Shell Backdoor Detection'. The description states: '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.' The solution advises: 'Verify if the remote host has been compromised, and reinstall the system if necessary.' The output section shows a successful execution of the 'id' command, resulting in root access. A table at the bottom lists the affected hosts, showing IP 192.168.1.10.

Vulnerabilities

CRITICAL Bind Shell Backdoor Detection

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.

Output
Nessus was able to execute the command "id" using the following request :

This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitabier/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitabier/#
----- snip -----

To see debug logs, please visit individual host

Port	Hosts
1524 / rdp / rdp_shell	192.168.1.10

Plugin Details

Severity: Critical
ID: 51988
Version: 1.10
Type: remote
Family: Backdoors
Published: February 15, 2011
Modified: April 11, 2022

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/CN:N/HA:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

è una porta di shell bind in ascolto su una porta remota senza alcuna autenticazione richiesta. Ciò significa che un utente malintenzionato può connettersi alla porta remota ed eseguire qualsiasi comando desiderato. Per correggere la vulnerabilità, è necessario disabilitare la porta di shell bind. Ciò può essere fatto modificando la configurazione del servizio che sta in ascolto sulla porta.