



Al fine della scansione è stato generato anche un report con le vulnerabilità.

My Basic Network Scan / Plugin #46882

Configure Audit Trail

Back to Vulnerabilities

Hosts 1 Vulnerabilities 64 Remediations 3 History 1

CRITICAL UnrealIRCd Backdoor Detection

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also
<https://seclists.org/fulldisclosure/2010/Jun/277>
<https://seclists.org/fulldisclosure/2010/Jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output

Prendiamo come esempio questa criticità UnrealIRCd Backdoor Detection

Aprendo il primo link possiamo dedurre che la versione 3.2.8.1 di UnrealIRCd è stata compromessa con una backdoor, come rivelato da una comunicazione inviata alla lista di distribuzione "irc-security". Questo errore consente a un aggressore di eseguire comandi arbitrari sul sistema ospitante il server IRC, ponendo a rischio la sicurezza e la privacy degli utenti.

My Basic Network Scan / Plugin #61708

ConfigureAudit Trail

Back to Vulnerabilities

Hosts1Vulnerabilities64Remediations3History1

CRITICALVNC Server 'password' 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.

Output

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.49.101

Analizziamo quest altro errore critico, VNC Server 'password' Password

In pratica, ci dice che il server VNC è protetto da una password debole, in quanto quest'ultima è 'password' ed un attaccante potrebbe facilmente entrare.

Per risolvere l'errore è consigliabile: Modificare immediatamente la password predefinita del server VNC utilizzando una password robusta e unica. La password dovrebbe essere lunga, complessa e contenere una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali.

My Basic Network Scan / Plugin #11356

ConfigureAudit Trail

[Back to Vulnerabilities](#)

Hosts1

Vulnerabilities64

Remediations3

History1

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
- dev
more...

To see debug logs, please visit individual host

Port ▼

Hosts

Osservando questa criticità (NFS Exported Share Information Disclosure) osserviamo che almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere “montato” dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

Per risolvere questo errore è consigliabile: Modificare la configurazione di NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote. Questo può essere realizzato tramite l'implementazione di restrizioni di accesso basate su indirizzi IP o domini.