Analisi delle vulnerabilità e azioni di rimedio

Daniele Renga

Scansione 2

Rimozione della Backdoor Detection

51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

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.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

tcp/1524/wild_shell

Per prima cosa sono andato a verificare se sulla porta 1524 ci fosse attivo qualche servizio, visto come da ricerca ,la porta 1524 di solito è associata ad una bind shell backdoor.

La porta precedentemente era in ascolto tramite il processo xinetd con PID 4423, ho eseguito subito il comando Kill 4423 per far si che il processo terminasse subito

Poi ho eseguito il comando sudo nestat -tulnp | grep 1524 per verificare che il processo sia terminato e che la porta 1524 fosse chiusa, ovviamente a seguire la scansione con Nessus per verificare se la vulnerabilità fosse risolta.

Esito positivo da parte di Nessus