

VULNERABILITY ASSESSMENT

REPORT - METASPLOITABLE 2

INFORMAZIONI SU SCANSIONE

- ESEGUITO L' 8 MAGGIO 2023
- IP: 192.168.50.101
- MAC ADDRESS: 08:00:27:A0:26:54
- OS: LINUX KERNEL 2.6 on Ubuntu 8.04

VULNERABILITÀ

- CRITICAL 3
- HIGH 2
- MEDIUM 1
- INFO 31

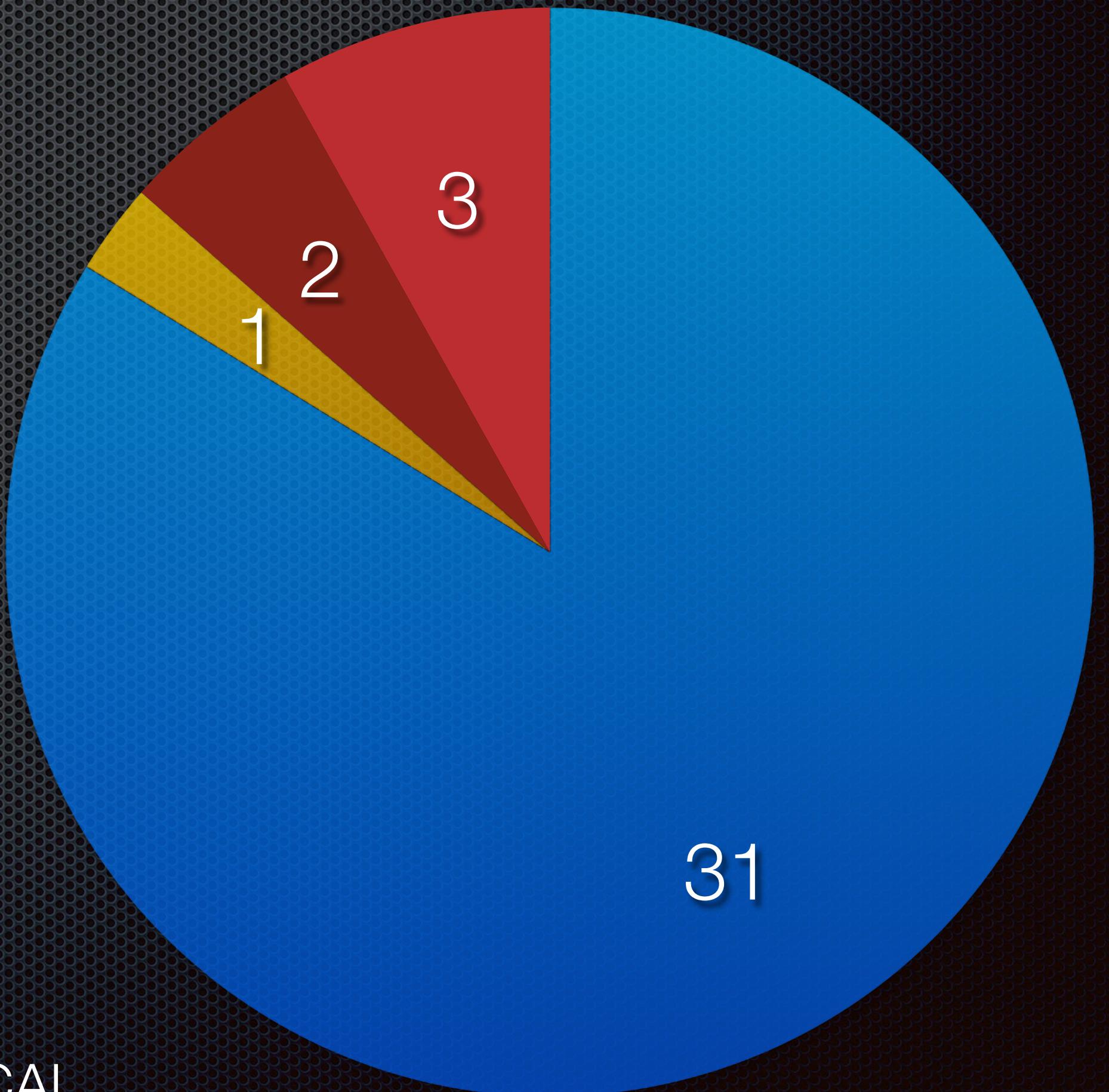
● INFO

● MEDIUM

● LOW

● LOW

● CRITICAL



VULNERABILITÀ CRITICHE

134862 Apache Tomcat AJP Connector Request Injection

È stata rilevata una vulnerabilità di lettura/inclusione di file in un connettore JP. Un utente malintenzionato, da remoto e non autenticato potrebbe leggere i file dell'applicazione ed ottenere la possibilità di far eseguire del codice arbitrario e malevolo alle macchine attaccate.

Si consiglia di aggiornare la configurazione di AJP ed il server Tomcat

Tempo ipotizzato per fixare il problema: 5 ore

VULNERABILITÀ CRITICHE

33850 Unix OS Unsupported Version Detection

Il sistema operativo non è più supportato.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto.

Si consiglia di aggiornare il SO ad una versione attualmente supportata

Tempo ipotizzato per fixare il problema: 5 ore

VULNERABILITÀ CRITICA

11356 NFS EXPORTED SHARE INFORMATION DISCLOSURE

È possibile accedere alle condivisioni NFS sull'host remoto.

Un utente malintenzionato potrebbe essere in grado di leggere e scrivere file sull'host remoto.

Si consiglia di configurare NFS in modo che solo gli host autorizzati possano utilizzare il servizio

Tempo ipotizzato per fixare il problema: 5 ore

VULNERABILITÀ ALTE

42256 NFS Shares World Readble

Il server NFS remoto esporta condivisioni leggibili da tutti, senza limitare l'accesso.

Si consiglia di configurare le restrizioni appropriate su tutte le condivisioni NFS.

Tempo ipotizzato per fixare il problema: 5 ore

VULNERABILITÀ ALTE

90509 Samba Badlock Vulnerability

La versione di Samba (server per Linux e Unix) è affetta da un difetto. Un attaccante rendendo visibili o modificare i dati sensibili presenti sul database.

Si consiglia di aggiornare la versione di Samba.

Tempo ipotizzato per fixare il problema: 5 ore

VULNERABILITÀ ALTE

12217 Dns Server Cache

Il server DNS è vulnerabile agli attacchi di snooping (prendere il controllo dell'identità di un'altra persona).

Gli attacchi sarebbero limitati alla sola rete interna.

Si consiglia di contattare il fornitore del software DNS per una correzione.

Tempo ipotizzato per fixare il problema: 2 ore