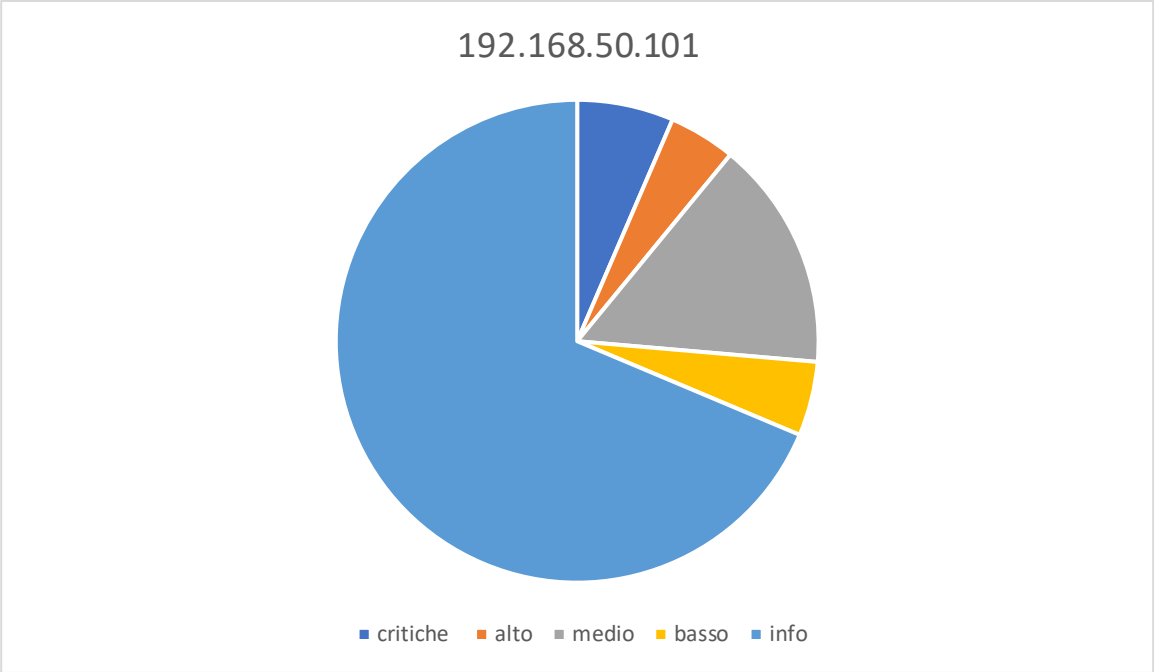

Inizio : 02/09/2023

Fine : 02/09/2023

Informazioni Host

Nome macchina : Metasploitable

IP : 192.168.50.101

OS : Debian (64 bit)

Vulnerabilità

Divulgazioni di informazioni sulle azioni esportate NFS. Porta 2049/udp/rpc-nfs

Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto può essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere file su host remoto.

Soluzione

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possono montare le proprie condivisioni remote

Fattore di rischio

Critico

Vulnerabilità

VNC Server password. Porta 5900/tcp/vnc

Descrizione

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è in grado di accedere utilizzando l'autenticazione VNC e una password di "password". UN utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

Soluzione

Proteggi il servizio VNC con una password complessa.

Fattore di rischio

Critico

Vulnerabilità

Iniezione di Richiesta tramite connettore AJP di Apache Tomcat. Porta 8009/tcp/ajp13

Descrizione

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto non autenticato può fruttare questa vulnerabilità per leggere i file dell'applicazione Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE)

Soluzione

Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successiva.

Fattore di rischio

Critico