NESSUS REPORT

Consegna U2-S5-L4

Breve report delle vulnerabilità critiche scovate dal tool Nessus sulla macchina Metasploitable.

- **Apache Tomcat SEoL (<= 5.5.x)**
  Versione di Apache Tomcat non supportata installata sull'host remoto.
  La versione installata non è quindi più mantenuta dallo sviluppatore e non riceverà di conseguenza nessun aggiornamento di sicurezza.

  Possibile soluzione alla falla:
  eseguire subito l'aggiornamento ad una versione più recente.

- **Bind Shell Backdoor Detection**
  È presente sulla macchina host una shell in ascolto sulla porta tcp 1524 senza alcun controllo dell'autenticazione. Qualsiasi malintenzionato potrebbe eseguire ogni genere di comando senza aver bisogno di autorizzazioni e di conseguenza compromettere l'intera macchina.

  Possibile soluzione alla falla:
  eseguire un'approfondita analisi del sistema in questione e se necessario provvedere ad una totale reinstallazione della stessa.

- **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**
  È presente una falla nella libreria OpenSSL che si occupa della generazione delle chiavi SSH. È stata individuata una rimozione di parte del codice che si occupa di generare entropia durante la creazione delle suddette chiavi. Sfruttando questa falla un attaccante potrebbe impadronirsi della parte privata della chiave e sfruttarla per decifrare la sessione remota oppure usarla per eseguire un attacco di tipo man-in-the-middle.

  Possibile soluzione alla falla:
  dato che tutto il materiale protetto con la crittografia è da considerarsi facilmente decifrabile da un attaccante esterno, si consideri la necessità di criptarlo nuovamente. La problematica in questione è stata identificata in OpenVPN, SSH e nel protocollo SSL.

- **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**
  Il certificato x509 generato sul server SSL è stato generato da una macchina Ubuntu/Debian con una falla di sicurezza nelle librerie OpenSSL. Nel dettaglio all'interno del codice che si occupa della generazione casuale di numeri. Sfruttando questa falla un attaccante potrebbe impadronirsi della parte privata della chiave e sfruttarla per decifrare la sessione remota oppure usarla per eseguire un attacco di tipo man-in-the-middle.

  Possibile soluzione alla falla:
  dato che tutto il materiale protetto con la crittografia è da considerarsi facilmente decifrabile da un attaccante esterno, si consideri la necessità di criptarlo nuovamente. La problematica in questione è stata identificata in OpenVPN, SSH e nel protocollo SSL.

- **NFS Exported Share Information Disclosure**
  La falla permette l'accesso ai file sul server condivisi tramite NFS.
  L'NFS è un file system che consente a computer client di utilizzare la rete per accedere a directory condivise da server remoti come fossero disponibili in locale. Un attaccante potrebbe leggere e probabilmente anche modificare dei fil presenti sulla macchina.

  Possibile soluzione alla falla:
  è necessario configurare il tutto affinché per accedere ai file condivisi serva un'autorizzazione.

- **SSL Version 2 and 3 Protocol Detection**
  La macchina utilizza dei protocolli di crittografia con delle criticità note. Vengono infatti accettate connessioni criptate con SSL in versione 2.0/3.0 che tra le tante falle annovera anche: uno schema di padding poco sicuro con CBC (block cipher mode), schemi di rinegoziazione/ripresa di sessione insicuro. Un attaccante potrebbe exploitare queste vulnerabilità per eseguire un attacco man-in-the-middle o peer decriptare le comunicazioni tra client e server. Nonostante sia notoriamente consigliato l'utilizzo delle versioni più recenti di SSL e TLS, alcuni browsers ancora integrano e supportano le vecchie versioni e ciò non fa altro che semplificare la vita dei malintenzionati che possono sfruttarli per abbassare la sicurezza del protocollo di connessione. Sarebbe

necessario disabilitare in toto questi protocolli ormai obsoleti. Il NIST (Istituto Nazionale degli Standard e Tecnologie) ha stabilito che non è più ammissibile definire sicure le connessioni criptate per mezzo di SSL 3.0.

Possibile soluzione alla falla:
Si consiglia di consultare la documentazione dell'applicazione per disabilitare l'uso di SSL 2.0/3.0. Si raccomanda l'uso di TLS 1.2 o versione superiore.

- **Unix Operating System Unsupported Version Detection**
  Il sistema operativo di tipo Unix della macchina risulta ormai obsoleto. Ciò implica il fatto che esso non riceverà più le correzioni di sicurezza necessarie al suo corretto funzionamento. Di conseguenza le vulnerabilità presenti non verranno mai risolte esponendo la macchina ad ogni genere di rischio esterno.

  Possibile soluzione alla falla:
  eseguire al più presto un aggiornamento ad una versione correttamente mantenuta e supportata.

- **UnrealIRCd Backdoor Detection**
  Il server IRC eseguito sulla macchina è una versione di UnrealIRCd corrotta da una backdoor che permette l'accesso non autorizzato alla macchina per l'esecuzione di codice malevolo da parte di un malintenzionato.

  Possibile soluzione alla falla:
  scaricare e reinstallare il software in questione previa verifica del checksum MD5/SHA1.

- **VNC Server 'password' Password**
  È presente un server VNC portato da una password troppo debole. Un attaccante potrebbe avere acceso remoto alla macchina facilmente.

  Possibile soluzione alla falla:
  Al posto di 'password' usare una password molto lunga e con tipi di carattere differenti.