Relazione S5L4
vulnerabilità individuate da Nessus

Lo scopo di questa relazione è quello di analizzare le prime quattro vulnerabilità critiche individuate da Nessus e spiegare in cosa consistono.

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Apache Tomcat è un server web che implementa le JSP (JavaServer Pages). La vulnerabilità in particolare è stata riscontrata sul connettore AJP che è un componentne necessario per integrare Tomcat in un'installazione di Apache.
Il problema sta nel fatto che un eventuale attaccante riesca ad accedere al server senza essere autenticato, in modo tale che possa aver accesso a contenuti sensibili o anche eseguire l'upload di codice malevolo tramite le JSP.

Bind Shell Backdoor Detection

Questa vulnerabilità critica ci segnala invece che è presente una shell bindata (collegata) ad una porta in ascolto su una porta. Chiunque riesca ad accedere alla shell potrà lanciare comandi sulla macchina senza bisogno di autenticazione.

SSL Version 2 and 3 Protocol Detection

Ci viene segnalato che la versione del protocollo SSL utilizzata ha delle falle di sicurezza crittografiche.
Un attaccante potrà sfruttare queste falle eseguendo un attacco man-in-the-middle oppure potrà decifrare la comunicazione tra client e server (la vulnerabilità più nota è POODLE).

Apache Tomcat SEoL (<= 5.5.x)

Il problema di questa vulnerabilità risiede nella versione in uso che non è più supportata/mantenuta dal produttore. Questo implica che non ci saranno più aggiornamenti e quindi se ci sono problemi di sicurezza non verranno fixati.

Davide Lecci