

UTILIZAÇÃO DA BIBLIOTECA STAGEFRIGHT PARA ACESSO PRIVILEGIADO EM DISPOSITIVOS COM SISTEMAS ANDROID

DEMITROV, Jessica Nascimento¹ SCATENA, Jean Miler²

Com a disseminação dos dispositivos móveis, temos uma nova área de pesquisa que visa à segurança desses dispositivos, que estão conectados na internet. Sendo assim, o presente trabalho tem como objetivo utilizar a biblioteca Stagefright, que é encontrada no gerenciador de multimídia dos sistemas Android, para realizar o carregamento de uma ferramenta de acesso remoto (Remote Access Tool-R.A.T.) que permitirá acesso externo privilegiado. Essa metodologia é baseada na prova de conceito (Proof of Concept) que visa fraudar o gerenciador de mídia do Android, através de um arquivo MP4 com o cabeçalho modificado. O arquivo contém uma pilha de controle que será utilizada para gerar a sobrecarga de uma determinada área da memória, permitindo que no processo de pré-carregamento do conteúdo, seja possível o carregamento e a execução de um R.A.T. Nessa prova de conceito será utilizada a vulnerabilidade (CVE) 2015-3864.

¹ Universidade Paulista - UNIP

² Fafra- Ituverava, Universidade Paulista - Ribeirão Preto e Fatec Mococa
