CFG란

CFG란 Control Flow Guard로 고도로 최적화 된 플랫폼 보안 기능이다. 해당 기능은 memory corruption 취약점을 없애기 위해 만들어 졌다. 응용 프로그램에서 실행가능한 코드의 위치를 엄격하게 제한해 buffer overflow취약점을 통해 임의의 코드를 실행하는 것을 어렵게 한다.

CFG가 동작하는방식은, 소프트웨어 취약점은 실행중인 프로그램에 극단적인 데이터가 들어감으로써 공격이 된다. 예를 들어 의도한 것보다 더 많은 데이터를 넣음으로 써 BOF가 발생하게 되는데 이것은 프로그램에 할당된 영역을 넘어가서 실행이 된다. 하지만 CFG는 컴파일 그리고 ㄹㄴ타임을 지원하고 둘의 강력한 조합은 간접 호출 명령어를 실행할 수 있는 위치를 엄격하게 제어하므로 써 무결성을 구현한다.

우회기법

해당 CFG를 우회하는 기법으로는 코드인젝션으로 외부입력을 통해 악성코드를 주입하여 프로그램의 흐름을 변경하는기법과, 동적 로딩으로 프로그램이 샐행 중에 외부에 있는 모듈을 로드하여 실행하는 기법과 다른언어를 사용해 특정 동작을 수행시키는 기법이 있다.