In this thesis, we proposed a new type of vulnerability, namely, the memory pressure bugs. This type of vulnerability was triggered by failed memory allocation. Using the existing fuzzing methods, it is extremely hard to trigger this type of bugs. It is also extremely difficult to reproduce this type of bugs since reproducing the crashes requires the identical memory allocation to be failed, while the memory allocations in computer system are hard to predict in general. To trigger this type of bugs, we developed low memory simulation instrumentation tools to aid our fuzzer to detect memory pressure bugs in web browsers. To reproduce this type of bugs, we introduced precise memory pressure in JavaScript code. We solve the problem of premature allocation failure of memory pressure bug by leveraging on the memory fragmentation to reserve memory space for allocation before the target allocation. Three new vulnerabilities of memory pressure bugs were successfully found in the Internet explorer.