Analysis of the bug

There is a stack-based buffer overflow in child(): `MAX_CMD` bytes are read into a `MAX_ARG`-sized array.