

HODOR: Shrinking Attack Surface on Node.js via System Call Limitation

Wenya Wang
Shanghai Jiao Tong University
Shanghai, China
duky_97@sjtu.edu.cn

Xingwei Lin
Ant Group
Hangzhou, China
xwlin.roy@gmail.com

Jingyi Wang*
Zhejiang University
ZJU-Hangzhou Global Scientific and
Technological Innovation Center
Hangzhou, China
wangjyee@zju.edu.cn

Wang Gao
Shanghai Jiao Tong University
Shanghai, China
gaowang.sjtu@gmail.com

Dawu Gu
Shanghai Jiao Tong University
Shanghai, China
dwgu@sjtu.edu.cn

Wei Lv
Ant Group
Hangzhou, China
huaxing.lw@antgroup.com

Jiashui Wang
Zhejiang University, Ant Group
Hangzhou, China
jiashui.wjs@antgroup.com

*Corresponding authors: Jingyi Wang and Dawu Gu

Table 9: Engine-required system calls.

Thread Type	Engine-required System Call
Main Thread	mprotect; futex; rt_sigaction; munmap; read; fstat; getpid; open; ioctl; rt_sigprocmask; stat; fcntl; writev; epoll_pwait; pread64; dup3; close; write; getcwd; getdents64; rt_sigreturn; brk; shutdown; statx; readlink; madvise; exit_group; epoll_ctl; mmap;
Thread Pool	read; futex; openat; socket; statx; open; exit; close; write; rt_sigprocmask; fcntl; getcwd; madvise; munmap; mmap;