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

Wenya Wang
Shanghai Jiao Tong University
Shanghai, China
ducky_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 8: Vulnerability payloads.

Critical Syscall		JavaScript	C*
Cmd Execution	**exec**	child_process.exec	execve
	fork	child_process.fork	fork
Permission	**setgit**	process.setuid	setuid
	setuid	process.setgid	setgid
Network	**bind**	net.connect	bind
	connect	dgram.createSocket.bind	connect
	listen	server.listen	listen

*: We compile the C code into binary and execute the binary as a shell.