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 6: Exploit execution for packages with arbitrary command execution attacks.

Package Name	Initial Attack	HODOR							
		Initial Attack	Cmd		Permission			Net	
			Exec	Fork	Setgid	Setuid	Connect	Listen	Bind
command-exists	Write command-exists	✔	✘	✘	✔	✔	✘	✔	✔
kill-by-port	Write success	✔	✘	✘	✔	✔	✔	✔	✔
killport	Write success	✔	✘	✘	✔	✔	✔	✔	✔
kill-process-by-name	Write success	✔	✘	✘	✔	✔	✔	✔	✔
macaddress	Write /tmp/poof	✔	✘	✘	✔	✔	✔	✔	✔
mc-kill-port	Write newFile.txt	✔	✘	✘	✔	✔	✘	✔	✔
onion-oled-js	Write success	✔	✘	✘	✔	✔	✔	✔	✔
open	Write /tmp/tada	✔	✘	✘	✔	✔	✔	✔	✔
pdf-image	Write /tmp/hacked	✔	✘	✘	✔	✔	✔	✔	✔
pdfinfojs	Write a	✔	✘	✘	✔	✔	✔	✔	✔
pidusage	Execute /usr/local/bin/python	✔	✘	✘	✔	✔	✔	✔	✔
portkiller	Write success	✔	✘	✘	✔	✔	✔	✔	✔
port-killer	Write success	✔	✘	✘	✔	✔	✘	✔	✔
portprocesses	Write success	✔	✘	✘	✔	✔	✔	✔	✔
ps	Write success.txt	✔	✘	✘	✔	✔	✔	✔	✔
ps-kill	Write success	✔	✘	✘	✔	✔	✔	✔	✔
ps-visitor	Write success	✔	✘	✘	✔	✔	✔	✔	✔
roar-pidusage	Write success	✔	✘	✘	✔	✔	✔	✔	✔
samsung-remote	Write /tmp/malicious;	✔	✘	✘	✔	✘	✔	✔	✔
scp	nc localhost 4444;	✔	✘	✘	✔	✔	✔	✔	✔
whereis	Write /tmp/tada	✔	✘	✘	✔	✔	✔	✔	✔
wincred	Write success	✔	✘	✘	✔	✔	✔	✔	✔
git-pull-or-clone	Write /tmp/pwn3	✔	✘	✘	✔	✔	✘	✔	✔
adb-driver	Write a	✔	✘	✘	✔	✔	✔	✔	✔
alfred-workflow-nodejs	Write hacked	✔	✘	✘	✔	✔	✔	✔	✔
apex-publish-static-files	Write apex-publish-static-files	✔	✘	✘	✔	✔	✘	✔	✔
apiconnect-cli-plugins	Write Song	✔	✘	✘	✔	✔	✔	✔	✔
async-git	Write HACKED #	✔	✘	✘	✘	✘	✘	✘	✘
bestzip	Write bestzip	✔	✘	✘	✔	✔	✔	✔	✔
blamer	Write vulnerable	✔	✘	✘	✔	✔	✔	✔	✔
cd-messenger	Write JHU	✔	✘	✘	✔	✔	✘	✔	✔
clamscan	Write create.txt	✔	✘	✘	✔	✔	✘	✔	✔
cocos-utils	Write hacked	✔	✘	✘	✔	✔	✔	✔	✔
codecov	Write codecov	✔	✘	✘	✔	✔	✘	✔	✔
compass-compile	Write JHU	✔	✘	✘	✔	✔	✔	✔	✔
connection-tester	Write 111	✔	✘	✘	✔	✔	✘	✔	✔
curling	Write JHU	✔	✘	✘	✔	✔	✔	✔	✔
curljs	Write JHU	✔	✘	✘	✔	✔	✔	✔	✔
deferred-exec	Write JHU	✔	✘	✘	✔	✔	✔	✔	✔
diskstats	Write HACKED	✔	✘	✘	✔	✔	✔	✔	✔
diskusage-ng	Write Song	✔	✘	✘	✔	✔	✔	✔	✔
docker-compose-remote-api	Write vulnerable.txt	✔	✘	✘	✔	✔	✘	✘	✘
enpeem	Write create.txt	✔	✘	✘	✔	✔	✔	✔	✔
eslint-fixer	Write eslint-fixer	✔	✘	✘	✘	✘	✔	✔	✔
ffmpegdotjs	Write success	✔	✘	✘	✔	✔	✔	✔	✔
ffmpeg-sdk	Write success	✔	✘	✘	✔	✔	✔	✔	✔
find-process	Write /tmp/semicolon_file	✔	✘	✘	✔	✔	✔	✔	✔
freespace	Write /tmp/semicolon_file	✔	✘	✘	✔	✔	✘	✔	✔
geojson2kml	Write JHU	✔	✘	✘	✔	✔	✔	✔	✔
git-add-remote	Write Song	✔	✘	✘	✔	✔	✘	✔	✔
gitblame	Write JHU	✔	✘	✘	✔	✔	✔	✔	✔
git-dummy-commit	Write git-dummy-commit	✔	✘	✘	✔	✔	✘	✔	✔
giting	Write create.txt	✔	✘	✘	✔	✔	✔	✔	✔
git-interface	Write /tmp/pwned	✔	✘	✘	✔	✔	✔	✔	✔
git-tags-remote	Write /tmp/command-injection.test	✔	✘	✘	✔	✔	✔	✔	✔
google-cloudstorage-commands	Write JHU	✔	✘	✘	✔	✔	✔	✔	✔
growl	Write aaaa	✔	✘	✘	✔	✔	✔	✔	✔
gry	Write HACKED	✔	✘	✘	✔	✔	✔	✔	✔
gulp-scss-lint	Write create.txt	✔	✘	✘	✔	✔	✘	✘	✘
gulp-styledocco	Write Vulnerable	✔	✘	✘	✔	✔	✘	✘	✘
gulp-tape	Write JHU.txt	✔	✘	✘	✘	✘	✘	✘	✘
heroku-env	Write JHU	✔	✘	✘	✘	✘	✔	✔	✔
im-metadata	Write im-metadata	✔	✘	✘	✘	✘	✘	✘	✘
im-resize	Write create.txt	✔	✘	✘	✔	✔	✔	✔	✔
install-package	Write Song	✔	✘	✘	✔	✔	✔	✔	✔
jison	Write pwned	✔	✘	✘	✔	✔	✔	✔	✔
killing	Write success	✔	✘	✘	✔	✔	✔	✔	✔
kill-port-process	Write kill-port-process	✔	✘	✘	✔	✔	✘	✔	✔
libnmap	Write success.txt	✔	✘	✘	✔	✔	✔	✔	✔
local-devices	Makek directory attacker	✔	✘	✘	✔	✔	✔	✔	✔
lsof	Write create.txt	✔	✘	✘	✘	✘	✔	✔	✔
lycwed-spritesheetjs	Write 111233 #	✔	✘	✘	✔	✔	✔	✔	✔
macfromip	Write JHU2	✔	✘	✘	✔	✘	✔	✔	✔
monorepo-build	Write JHU	✔	✘	✘	✔	✔	✘	✔	✔
network-manager	Write create.txt	✔	✘	✘	✔	✔	✘	✔	✔
node-df	Write HACKED	✔	✘	✘	✔	✔	✔	✔	✔
node-key-sender	Write Song	✔	✘	✘	✔	✔	✔	✔	✔
node-latex-pdf	Write JHU	✔	✘	✘	✘	✘	✘	✘	✘
node-mpv	Write JHU	✔	✘	✘	✔	✔	✘	✔	✔
node-prompt-here	Write create.txt	✔	✘	✘	✔	✔	✘	✔	✔
node-ps	Write JHU	✔	✘	✘	✔	✔	✔	✔	✔
node-unrar	Write node-unrar	✔	✘	✘	✔	✔	✔	✔	✔
npm-lockfile	Write rce	✔	✘	✘	✔	✔	✔	✔	✔
psnode	Write success	✔	✘	✘	✔	✔	✔	✔	✔
pulverizr	Write Song	✔	✘	✘	✔	✔	✔	✔	✔
react-dev-utils	Write react-dev-utils	✔	✘	✘	✔	✔	✘	✔	✔
rpi	Write vulnerable.txt	✔	✘	✘	✔	✔	✔	✔	✔
serial-number	Write create.txt	✔	✘	✘	✘	✘	✔	✔	✔
strider-git	Write HACKED;	✔	✘	✘	✘	✘	✘	✘	✘
strong-nginx-controller	Write Song	✔	✘	✘	✔	✔	✔	✔	✔
theme-core	Write JHU	✔	✘	✘	✔	✔	✔	✔	✔
ts-process-promises	Write JHU	✔	✘	✘	✔	✔	✔	✔	✔
umount	Write Song	✔	✘	✘	✘	✘	✔	✔	✔
vboxmanage.js	Write HACKED	✔	✘	✘	✔	✔	✔	✔	✔

wc-cmd	**Write JHU**	✔	✘	✘	✔	✔	✔	✔	✔
wifiscanner	**Write /tmp/exploit.txt**	✔	✘	✘	✔	✔	✔	✔	✔
xopen	**Write JHU**	✔	✘	✘	✔	✔	✔	✔	✔
xps	**Write HACKED**	✔	✘	✘	✔	✔	✔	✔	✔
aaptjs	**Write aaptjs**	✔	✘	✘	✘	✘	✘	✘	✘
arpping	**Write HACKED**	✔	✘	✘	✔	✔	✔	✔	✔
dns-sync	**Write pwned**	✔	✘	✘	✔	✔	✘	✔	✔
git	**date**	✘	✘	✘	✔	✔	✘	✔	✔
git-lib	**Write HACKED;**	✔	✘	✘	✔	✔	✔	✔	✔
git-parse	**Write HACKED**	✔	✘	✘	✔	✔	✔	✔	✔
gity	**Write HACKED**	✔	✘	✘	✔	✔	✔	✔	✔
imagickal	**Write HACKED**	✔	✘	✘	✔	✔	✔	✔	✔
meta-git	**Write HACKED**	✔	✘	✘	✔	✔	✔	✔	✔
node-os-utils	**Write DUMMY_FILE**	✔	✘	✘	✔	✔	✘	✔	✔
pomelo-monitor	**Write Song**	✔	✘	✘	✔	✔	✔	✔	✔
gm	**Write gm**	✔	✘	✘	✔	✔	✔	✔	✔

✘: Exploits are executed; ✔: Exploits are blocked;