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 7: Exploit execution for packages with arbitrary code execution attacks.

Package Name	Initial Attack	HODOR								MIR							
			Cmd		Permission		Net				Cmd		Permission		Net		
		Initial Attack	Exec	Fork	Setgid	Setuid	Connect	Listen	Bind	Initial Attack	Exec	Fork	Setgid	Setuid	Connect	Listen	Bind
accesslog	Print xSS	✘	✔	✔	✔	✔	✔	✔	✔				/				
access-policy	Print 123	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
adm-zip	Path traversal	✔	✔	✔	✔	✔	✔	✔	✔				/				
angular-expressions	Write file angular-expressions-success	✔	✔	✔	✔	✔	✔	✔	✔				/				
cd-messenger	Print JHU	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
cryop	Print defconrussia	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
djv	touch HACKED	✔	✔	✔	✔	✔	✔	✔	✔				/				
ejs	Write file ejs-success	✔	✔	✔	✔	✔	✔	✔	✔				/				
eslint-utils	Write file eslint-utils-success	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
front-matter	Print 1	✘	✔	✔	✔	✔	✔	✔	✔				/				
grunt	Returns Date.now	✔	✘	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
hot-formula-parser	Write file test	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
is-my-json-valid	Execute cat /etc/passwd	✔	✔	✔	✔	✔	✔	✔	✔				/				
jsen	Write file malicious	✔	✘	✘	✘	✘	✘	✘	✘				/				
js-yaml	Returns Date.now	✔	✔	✔	✔	✔	✔	✔	✔				/				
kmc	Write file kmc-success	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
marsdb	Write file marsdb-success	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
metacalc	Print process	✘	✔	✔	✔	✔	✔	✔	✔				/				
mixin-pro	Print hacked	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
m-log	Print injected	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
mock2easy	Write mock2easy-success	✘	✔	✔	✔	✔	✘	✘	✘	✔	✔	✔	✔	✔	✔	✔	✔
modjs	Write modjs-success.txt	✘	✘	✘	✔	✔	✘	✘	✘	✔	✔	✔	✔	✔	✔	✔	✔
modulify	Print hacked	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
mol-proto	Write file mol-proto-success	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
mongodb-query-parser	touch test-file	✔	✔	✔	✔	✔	✘	✘	✘				/				
mongo-express	exec calculator	✔	✔	✔	✔	✔	✔	✔	✔				/				
mongoosemask	Print "my evil code was run"	✘	✔	✔	✔	✔	✔	✔	✔				/				
mongo-parse	Write file hacked	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
morgan	Write file mongui-success	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
morgan-json	Print GLOBAL CTF HIT	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
mosc.js	Write file Song	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
node-extend	Print 123	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
node-extend	Print 123	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
node-rules.js	Print 123	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
node-serialize	Execute ls	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
notevil	Print pwned	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
pg	Print process.env	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
pixl-class	Print 123	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
post-loader	Print rce	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
protojs	Write file protojs-success	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
realms-shim	Messed with Object.toString	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
reduce-css-calc	Read /etc/passwd	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
safe-eval	Return proces	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
safer-eval	Print id	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
sandbox	Print process.pid	✘	✘	✘	✔	✔	✔	✔	✔	✔	✘	✘	✔	✔	✔	✔	✔
serialize-javascript	Print 1	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
serialize-to-js	Execute ls	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
static-eval	Print hacked	✔	✘	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
tar	Overwrite file	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
thenify	Write file Song	✔	✔	✔	✔	✔	✔	✔	✔				/				
total.js	Touch HACKED	✘	✔	✔	✔	✔	✘	✘	✘				/				
total4	Touch HACKED	✔	✘	✘	✔	✔	✘	✘	✘				/				
typed-function	Execute whoami	✔	✔	✔	✔	✔	✔	✔	✔				/				
underscore	touch HELLO	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
value-censorship	Access the Function constructor	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
vm2	return process.env	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
zhaoyao91-eval-in-vm	return process.env	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
mobile-icon-resizer	Print hacked	✘	✘	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

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