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 5: HODOR granularity of packages at system call level and thread level (RQ1).

Attack Type	CVE	Package Name	Node.js with Musl Libc		Hodor		Node.js with Musl Libc		Hodor		# of CL	% of CL-1	% of CL-2
			# of CS	# of TS	# of CS	# of TS	# of MT	# of TP	# of MT	# of TP			
Arbitrary Command Injection	/	command-exists	10	95	7	74	105	87	80	34	47	74.60%	74.60%
Arbitrary Command Injection	CVE-2021-23363	kill-by-port	10	93	3	57	103	0	60	0	6	0.01%	85.71%
Arbitrary Command Injection	CVE-2021-23360	killport‡	11	99	11	72	110	0	83	0	237	18.53%	95.83%
Arbitrary Command Injection	CVE-2021-23356	kill-process-by-name	11	99	11	72	110	0	83	0	6	75.00%	75.00%
Arbitrary Command Injection	CVE-2018-13797	macaddress	10	93	5	58	103	0	63	0	52	36.36%	36.36%
Arbitrary Command Injection	CVE-2022-25973	mc-kill-port	10	95	7	74	105	87	80	33	405	34.40%	72.72%
Arbitrary Command Injection	CVE-2021-23377	onion-oled-js	10	93	3	57	103	0	60	0	145	10.11%	82.35%
Arbitrary Command Injection	/	open	10	93	3	57	103	0	60	0	12	47.82%	47.82%
Arbitrary Command Injection	CVE-2018-3757	pdf-image‡	11	99	11	75	110	87	85	34	194	25.19%	86.15%
Arbitrary Command Injection	CVE-2018-3746	pdfinfojs	10	93	4	60	103	87	62	34	535	15.06%	100.00%
Arbitrary Command Injection	CVE-2017-1000220	pidusage‡	10	93	3	57	103	0	60	0	68	62.96%	62.96%
Arbitrary Command Injection	CVE-2021-23379	portkiller‡	10	93	3	57	103	0	60	0	12	88.23%	88.23%
Arbitrary Command Injection	CVE-2021-23359	port-killer	10	95	7	72	105	0	79	0	8	100.00%	100.00%
Arbitrary Command Injection	CVE-2021-23348	portprocesses‡	10	93	3	57	103	0	60	0	19	88.57%	88.57%
Arbitrary Command Injection	CVE-2018-16460	ps	10	93	3	57	103	0	60	0	28	75.00%	75.00%
Arbitrary Command Injection	CVE-2021-23355	ps-kill	11	99	11	72	110	0	83	0	3	12.50%	100.00%
Arbitrary Command Injection	CVE-2021-23374	ps-visitor	11	99	11	72	110	0	83	0	29	14.79%	76.68%
Arbitrary Command Injection	CVE-2021-23380	roar-pidusage‡	10	93	3	57	103	0	60	0	62	50.81%	70.81%
Arbitrary Command Injection	/	samsung-remote	11	99	11	75	110	87	85	34	27	56.52%	56.52%
Arbitrary Command Injection	/	scp	11	99	11	72	110	0	83	0	14	87.50%	87.50%
Arbitrary Command Injection	CVE-2018-3772	whereis‡	11	99	11	72	110	0	83	0	15	28.30%	83.33%
Arbitrary Command Injection	CVE-2021-23399	wincred	11	99	11	72	110	0	83	0	10	76.92%	76.92%
Argument Injection	CVE-2022-24437	git-pull-or-clone	10	95	9	75	105	87	82	36	177	31.72%	92.85%
Command Injection	CVE-2020-7636	adb-driver	11	99	11	73	110	87	83	33	66	39.75%	91.30%
Command Injection	/	alfred-workflow-nodejs	10	93	4	60	103	87	62	34	729	2.18%	86.95%
Command Injection	CVE-2018-16462	apex-publish-static-files	10	95	9	73	105	0	82	0	8	7.76%	7.76%
Command Injection	CVE-2020-7633	apiconnect-cli-plugins‡	10	93	3	57	103	0	60	0	19,230	8.83%	11.43%
Command Injection	CVE-2021-3190	async-git ‡	11	99	11	72	110	0	83	0	59	69.41%	74.19%
Command Injection	CVE-2020-7730	bestzip‡	11	99	11	82	110	87	92	35	4,204	12.60%	89.04%
Command Injection	CVE-2019-10807	blamer‡	10	93	3	57	103	0	60	0	1,465	13.88%	57.57%
Command Injection	CVE-2020-7795	cd-messenger	10	95	9	72	105	0	81	0	374	36.77%	83.33%
Command Injection	CVE-2020-7613	clamscan‡	10	93	6	56	103	87	57	35	2,493	8.16%	21.28%
Command Injection	/	cocos-utils	10	93	4	64	103	87	66	34	95	9.17%	9.17%
Command Injection	CVE-2020-15123	codecov	10	95	7	76	105	87	81	37	1,895	8.53%	8.53%
Command Injection	CVE-2020-7635	compass-compile	10	93	3	57	103	0	60	0	202	13.96%	95.65%
Command Injection	CVE-2020-7781TAB	connection-tester	10	95	9	72	105	0	81	0	43	68.25%	67.74%
Command Injection	CVE-2019-10789	curling	11	99	11	72	110	0	83	0	52	85.24%	85.24%
Command Injection	CVE-2020-28425	curljs	11	99	11	72	110	0	83	0	75	66.37%	78.12%
Command Injection	CVE-2020-28438	deferred-exec	11	99	11	72	110	0	83	0	1,339	9.93%	87.75%
Command Injection	/	diskstats‡	10	93	3	57	103	0	60	0	55	94.82%	94.82%
Command Injection	CVE-2020-7631	diskusage-ng	11	99	11	72	110	0	83	0	23	13.93%	32.39%
Command Injection	CVE-2020-7606	docker-compose-remote-api	11	99	9	75	110	87	83	35	1,143	10.99%	88.88%
Command Injection	CVE-2019-10801	enpeem	11	99	11	72	110	0	83	0	84	65.62%	87.80%
Command Injection	CVE-2021-26275	eslint-fixer‡	11	99	11	72	110	0	83	0	5,629	10.41%	66.66%
Command Injection	CVE-2021-23376	ffmpegdotjs ‡	11	99	11	73	110	0	84	0	43	41.74%	36.95%
Command Injection	CVE-2021-23376	ffmpeg-sdk ‡	11	99	11	72	110	0	83	0	18	75.00%	75.00%
Command Injection	/	find-process‡	10	93	3	57	103	0	60	0	110	5.56%	42.96%
Command Injection	/	freespace‡	11	101	11	80	112	0	91	0	27	44.26%	59.09%
Command Injection	CVE-2020-28429	geojson2kml	10	93	3	57	103	0	60	0	6	100.00%	100.00%
Command Injection	CVE-2020-7630	git-add-remote	11	101	11	80	112	0	91	0	13	65.00%	65.00%
Command Injection	CVE-2020-28434	gitblame	11	99	11	72	110	0	83	0	9	18.00%	75.00%
Command Injection	CVE-2018-3785	git-dummy-commit	11	101	11	87	112	0	98	0	490	7.41%	88.88%
Command Injection	CVE-2019-10802	giting	11	99	11	73	110	87	83	34	197	20.02%	64.56%
Command Injection	CVE-2022-1440	git-interface	10	93	9	60	103	0	69	0	94	68.11%	68.11%
Command Injection	/	git-tags-remote‡	11	99	11	72	110	0	83	0	236	32.14%	100.00%
Command Injection	CVE-2020-28436	google-cloudstorage-commands‡	10	93	3	57	103	0	60	0	13	52.00%	52.00%
Command Injection	CVE-2017-16042	growl	10	93	9	61	103	0	70	0	35	45.45%	45.45%
Command Injection	CVE-2020-36650	gry	11	99	11	74	110	87	83	34	190	59.00%	88.23%
Command Injection	CVE-2020-7601	gulp-scss-lint‡	11	99	9	86	110	87	89	42	5,065	9.60%	40.54%
Command Injection	CVE-2020-7607	gulp-styledocco	11	99	11	86	110	87	91	44	664	1.30%	77.08%
Command Injection	CVE-2020-7605	gulp-tape	11	99	11	86	110	87	91	44	32	5.08%	84.21%
Command Injection	CVE-2020-28437	heroku-env	11	99	11	75	110	87	85	34	25	33.33%	42.00%
Command Injection	CVE-2019-10788	im-metadata	11	99	11	72	110	0	83	0	57	86.36%	83.72%
Command Injection	CVE-2019-10787	im-resize	10	93	3	57	103	0	60	0	85	19.63%	85.71%
Command Injection	CVE-2020-7629	install-package‡	11	99	11	72	110	0	83	0	42	93.33%	93.33%
Command Injection	CVE-2020-8178	jison	10	93	3	57	103	0	60	0	1,916	9.01%	61.24%
Command Injection	CVE-2021-23381	killing‡	11	99	11	72	110	0	83	0	38	9.76%	90.24%
Command Injection	CVE-2019-15609	kill-port-process	11	101	11	81	112	87	91	33	259	20.45%	56.75%
Command Injection	CVE-2018-16461	libnmap	11	99	11	74	110	87	83	34	3,069	6.30%	80.93%
Command Injection	/	local-devices	10	93	8	79	103	87	66	57	37	37.37%	55.73%
Command Injection	CVE-2019-10783	lsof	11	99	11	72	110	0	83	0	54	91.30%	91.30%
Command Injection	/	lycwed-spritesheetjs	10	93	4	61	103	87	63	35	1,715	34.02%	63.54%
Command Injection	CVE-2020-7786	macfromip	11	99	11	75	110	87	85	34	39	45.88%	45.88%
Command Injection	CVE-2020-28434	monorepo-build	10	95	7	72	105	0	79	0	7,810	7.58%	85.18%
Command Injection	CVE-2019-10786	network-manager	10	95	9	72	105	0	81	0	93	89.42%	93.00%
Command Injection	CVE-2019-15597	node-df	11	99	11	72	110	0	83	0	84	1.71%	91.30%
Command Injection	CVE-2020-7627	node-key-sender‡	11	99	11	72	110	0	83	0	93	77.50%	77.50%
Command Injection	CVE-2020-28433	node-latex-pdf	11	99	11	72	110	0	83	0	9	60.00%	60.00%
Command Injection	CVE-2020-7632	node-mpv	10	95	7	72	105	0	79	0	36	14.63%	14.63%
Command Injection	CVE-2020-7602	node-prompt-here	10	95	7	72	105	0	79	0	8	6.66%	57.14%
Command Injection	CVE-2020-7785	node-ps	11	99	11	72	110	0	83	0	37	75.51%	75.51%
Command Injection	/	node-unrar	11	99	11	72	110	0	83	0	17	8.21%	100.00%
Command Injection	CVE-2022-0841	npm-lockfile‡	10	93	3	57	103	0	60	0	1,963	7.01%	70.96%
Command Injection	CVE-2021-23375	psnode	11	99	11	72	110	0	83	0	63	6.12%	35.13%
Command Injection	CVE-2020-7604	pulverizr	11	99	11	77	110	87	87	33	614	6.56%	87.02%
Command Injection	CVE-2021-24033	react-dev-utils	10	95	9	72	105	0	81	0	6,425	11.77%	22.32%
Command Injection	CVE-2019-10796	rpi	11	99	11	72	110	0	83	0	28	65.11%	65.00%
Command Injection	CVE-2019-10804	serial-number	11	99	11	73	110	87	83	33	45	57.69%	57.69%
Command Injection	/	strider-git	11	99	11	77	110	87	87	36	464	24.82%	42.40%
Command Injection	CVE-2020-7621	strong-nginx-controller	10	93	3	57	103	0	60	0	17,994	6.37%	49.70%
Command Injection	CVE-2020-28432	theme-core‡	10	93	4	58	103	87	60	33	1,721	15.46%	81.35%
Command Injection	CVE-2020-7784	ts-process-promises	11	99	11	73	110	87	83	33	2,376	16.29%	84.76%%
Command Injection	CVE-2020-7628	umount	11	99	11	72	110	0	83	0	965	8.20%	71.73%
Command Injection	/	vboxmanage.js‡	11	99	11	75	110	87	85	34	55	25.82%	25.82%
Command Injection	CVE-2020-28431	wc-cmd‡	11	99	11	72	110	0	83	0	31	0.44%	82.50%
Command Injection	CVE-2020-15362	wifiscanner	11	99	11	73	110	87	83	33	215	9.10%	83.33%

Command Injection	**CVE-2020-28447**	**xopen‡**	11	99	11	72	110	0	83	0	9	90.00%	90.00%
Command Injection	**/**	**xps**	11	99	11	72	110	0	83	0	51	4.26%	54.54%
Remote Code Execution	**CVE-2020-36378**	**aaptjs**	11	101	11	87	112	0	98	0	457	13.00%	97.05%
Remote Code Execution	**/**	**arpping‡**	11	99	11	72	110	0	83	0	98	27.68%	78.40%
Remote Code Execution	**CVE-2020-11079**	**dns-sync‡**	11	101	11	83	112	87	93	35	344	27.80%	97.22%
Remote Code Execution	**CVE-2021-23632**	**git**	10	93	3	57	103	0	60	0	648	15.72%	15.89%
Remote Code Execution	**/**	**git-lib‡**	10	93	3	57	103	0	60	0	999	11.35%	59.02%
Remote Code Execution	**/**	**git-parse**	10	93	4	60	103	87	62	34	704	2.96%	39.51%
Remote Code Execution	**/**	**gity**	11	99	11	72	110	0	83	0	33	13.25%	55.93%
Remote Code Execution	**/**	**imagickal‡**	11	99	11	75	110	87	85	35	1,183	13.13%	83.16%
Remote Code Execution	**/**	**meta-git‡**	10	93	3	57	103	0	60	0	355	8.32%	89.02%
Remote Code Execution	**/**	**node-os-utils‡**	10	95	7	72	105	0	79	0	172	47.77%	47.77%
Remote Code Execution	**CVE-2020-7620**	**pomelo-monitor**	10	93	3	58	103	0	61	0	90	86.53%	86.53%
Remote Shell Command Injection	**CVE-2015-7982**	**gm‡**	10	93	3	57	103	0	60	0	675	49.52%	58.50%
Arbitrary Code Execution	**CVE-2020-7729**	**grunt**	11	98	5	67	109	87	70	33	6,747	7.69%	47.13%
Arbitrary Code Execution	**/**	**is-my-json-valid**	1	28	1	28	29	0	29	0	3,560	9.92%	93.84%
Arbitrary Code Execution	**CVE-2020-7777**	**jsen**	11	99	11	72	110	0	83	0	766	34.56%	95.15%
Arbitrary Code Execution	**CVE-2020-7673**	**node-extend**	1	28	1	28	29	0	29	0	24	82.75%	82.75%
Arbitrary Code Execution	**CVE-2017-16082**	**pg**	1	28	1	28	29	0	29	0	260	12.26%	27.54%
Arbitrary Code Execution	**CVE-2020-7640**	**pixl-class**	1	28	1	28	29	0	29	0	38	79.16%	79.16%
Arbitrary Code Execution	**CVE-2022-0748**	**post-loader**	6	83	1	40	89	0	41	0	900	8.64%	69.23%
Arbitrary Code Execution	**/**	**serialize-to-js**	1	28	1	28	29	0	29	0	120	5.10%	86.33%
Arbitrary Code Execution	**CVE-2021-23389**	**total.js**	6	83	2	46	89	87	44	35	2,072	6.55%	6.55%
Arbitrary Code Execution	**CVE-2021-23390**	**total4**	10	94	5	72	104	87	75	38	1,874	6.79%	6.79%
Arbitrary Code Execution	**CVE-2017-1001004**	**typed-function**	1	28	1	28	29	0	29	0	397	74.62%	74.62%
Arbitrary Code Injection	**/**	**kmc**	6	83	1	45	89	0	46	0	2,267	6.02%	55.81%
Arbitrary Code Injection	**/**	**marsdb**	1	28	1	28	29	0	29	0	1,825	18.20%	54.06%
Arbitrary Code Injection	**/**	**mixin-pro**	1	28	1	28	29	0	29	0	78	82.10%	82.10%
Arbitrary Code Injection	**/**	**m-log**	1	28	1	28	29	0	29	0	289	0.88%	100.00%
Arbitrary Code Injection	**/**	**mobile-icon-resizer**	10	93	4	59	103	87	61	35	54	33.75%	65.51%
Arbitrary Code Injection	**/**	**mock2easy**	10	93	5	70	103	87	73	35	/	/	/
Arbitrary Code Injection	**/**	**modjs**	10	93	4	62	103	87	64	34	167	2.11%	6.77%
Arbitrary Code Injection	**/**	**modulify**	6	83	1	40	89	0	41	0	1,133	1.97%	80.70%
Arbitrary Code Injection	**/**	**mol-proto**	1	28	1	28	29	0	29	0	403	90.76%	90.76%
Arbitrary Code Injection	**/**	**mongoosemask**	1	28	1	28	29	0	29	0	50	19.92%	67.56%
Arbitrary Code Injection	**/**	**protojs**	1	28	1	28	29	0	29	0	132	10.09%	90.76%
Arbitrary Code Injection	**CVE-2020-7660**	**serialize-javascript**	1	28	1	28	29	0	29	0	71	5.10%	93.42%
Arbitrary File Overwrite	**CVE-2021-32803**	**tar**	6	83	3	56	89	87	57	48	7,830	11.69%	83.14%
Arbitrary File Write	**CVE-2018-1002204**	**adm-zip‡**	6	83	1	41	89	0	42	0	516	26.81%	26.84%
Code Execution	**CVE-2017-5941**	**node-serialize**	1	28	1	28	29	0	29	0	52	92.85%	92.85%
Code Injection	**CVE-2022-25760**	**accesslog**	6	83	1	43	89	0	44	0	95	41.48%	83.33%
Code Injection	**CVE-2020-7674**	**access-policy**	1	28	1	28	29	0	29	0	81	0.26%	96.42%
Code Injection	**CVE-2021-21277**	**angular-expressions**	1	28	1	28	29	0	29	0	713	48.01%	48.01%
Code Injection	**CVE-2020-7675**	**cd-messenger**	1	28	1	28	29	0	29	0	374	36.77%	90.69%
Code Injection	**CVE-2018-3784**	**cryop**	1	28	1	28	29	0	29	0	90	84.11%	84.11%
Code Injection	**CVE-2019-15657**	**eslint-utils**	6	83	2	50	89	87	48	35	436	8.92%	80.89%
Code Injection	**CVE-2021-23639**	**front-matter**	6	83	2	42	89	87	36	33	1,096	11.35%	80.95%
Code Injection	**CVE-2020-6836**	**hot-formula-parser**	1	28	1	28	29	0	29	0	1,650	6.25%	89.94%
Code Injection	**/**	**js-yaml**	1	28	1	28	29	0	29	0	1,753	19.62%	70.66%
Code Injection	**CVE-2022-21122**	**metacalc**	7	90	2	52	97	0	54	0	59	54.12%	86.95%
Code Injection	**CVE-2019-5413**	**morgan**	6	83	2	48	89	87	46	35	2,135	11.69%	81.48%
Code Injection	**CVE-2022-25921**	**morgan-json**	6	83	1	32	89	0	33	0	261	12.59%	94.11%
Code Injection	**CVE-2020-7672**	**mosc.js**	1	28	1	28	29	0	29	0	47	0.93%	88.67%
Code Injection	**CVE-2020-7609**	**node-rules.js**	1	28	1	28	29	0	29	0	939	40.57%	91.58%
Code Injection	**CVE-2016-10548**	**reduce-css-calc**	1	28	1	28	29	0	29	0	110	87.27%	87.27%
Code Injection	**CVE-2020-7677**	**thenify**	1	28	1	28	29	0	29	0	50	56.81%	82.14%
Prototype Pollution	**CVE-2020-7743**	**mathjs**	1	28	1	28	29	0	29	0	2,650	9.83%	8.52%
Prototype Pollution	**CVE-2021-23594**	**realms-shim**	6	83	1	38	89	0	39	0	1,118	3.59%	78.18%
Remote Code Execution	**/**	**djv**	1	28	1	28	29	0	29	0	300	33.44%	55.35%
Remote Code Execution	**/**	**mongodb-query-parser**	7	90	3	60	97	87	59	35	2,688	5.32%	28.49%
Remote Code Execution	**CVE-2019-10758**	**mongo-express**	6	83	2	43	89	87	42	33	9,225	11.46%	23.58%
Remote Code Execution	**CVE-2020-24391**	**mongo-parse**	1	28	1	28	29	0	29	0	342	83.82%	83.82%
Sandbox Breakout	**/**	**notevil**	1	28	1	28	29	0	29	0	2,828	9.68%	89.58%
Sandbox Breakout	**CVE-2019-10769**	**safer-eval**	7	90	2	52	97	0	54	0	119	35.31%	80.76%
Sandbox Breakout	**/**	**sandbox**	10	93	4	58	103	87	60	33	42	48.88%	48.88%
Sandbox Breakout	**/**	**static-eval**	11	99	9	74	110	87	82	34	2,891	7.69%	75.51%
Sandbox Breakout	**/**	**value-censorship**	7	90	2	52	97	0	54	0	3,089	8.43%	95.00%
Sandbox Bypass	**CVE-2019-10761**	**vm2**	7	90	2	52	97	0	54	0	50	0.09%	53.33%
Sandbox Escape	**CVE-2020-7710**	**safe-eval**	6	83	1	38	89	0	39	0	11	95.15%	95.15%
Sandbox Escape	**CVE-2020-7710**	**zhaoyao91-eval-in-vm**	6	83	1	38	89	0	39	0	7	100.00%	100.00%
Template Injection	**CVE-2022-29078**	**ejs**	6	83	1	40	89	0	41	0	32	5.22%	87.33%
Template Injection	**CVE-2021-23358**	**underscore**	1	28	1	28	29	0	29	0	239	48.38%	48.38%
Arbitrary Command Execution			**1,161**	**10,636**	**910**	**7,617**	**11,797**	**2,958**	**8,444**	**1,212**	**936**	35.61%	69.14%
Arbitrary Code Execution			**243**	**3,352**	**110**	**2,294**	**3,595**	**1,218**	**2,362**	**496**	**1,178**	30.83%	71.03%

CS: Critical system calls invocation;
TS: Trivial system calls invocation;
MT: Main Thread system calls invocation;
TP: Thread Pool system calls invocation;
‡: Packages that invoke system calls that are triggered by the execution of builtin methods;
CL: Covered line num of the package;
CL-1: Covered line of the package;
CL-2: Covered line of the package module;