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

Wenya Wang Shanghai Jiao Tong University Shanghai, China ducky_97@sjtu.edu.cn

Wang Gao Shanghai Jiao Tong University Shanghai, China gaowang.sjtu@gmail.com Xingwei Lin Ant Group Hangzhou, China xwlin.roy@gmail.com

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

Jiashui Wang Zhejiang University, Ant Group Hangzhou, China jiashui.wjs@antgroup.com Jingyi Wang*
Zhejiang University
ZJU-Hangzhou Global Scientific and
Technological Innovation Center
Hangzhou, China
wangjyee@zju.edu.cn

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

^{*}Corresponding authors: Jingyi Wang and Dawu Gu

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

| March Type | Attack Type |] | Package Name | Node,js with Musl Libc | | Hodor | | Node.js with Musl Libc | | Hodor | | I | 1 | |
|--|-------------------------------------|----------------------------------|---------------------------|------------------------|----------|-------|----------|------------------------|---------|----------|------|-----------|----------------|-------------------|
| Activity Communication CV-201-23-106 Mile Septem 10 94 11 72 110 10 10 10 10 10 10 | | CVE | | | | | | | | ' | | # of CL | % of CL-1 | % of CL-2 |
| Andreiry Command physicals An | | / | | | | | | | | | | | | 74.60% |
| Addition Command physics Addition Command phys | | | | | | | | | | | | | | 85.71% 95.83% |
| Arthory Command legislate | Arbitrary Command Injection | CVE-2021-23356 | kill-process-by-name | 11 | 99 | 11 | 72 | 110 | 0 | 83 | 0 | 6 | 75.00% | 75.00% |
| Adabasey Cassmall lighting Adabasey Cassmall lig | | | | | | | | | | | | | | 36.36% |
| Adabasey Camman liquidina Adabasey Camman li | | | | | | | | | | | | | | 72.72% 82.35% |
| Admirroy Cammal Injection Ca | | / | | | | 3 | 57 | | 0 | | 0 | 12 | | 47.82% |
| Arthony Cammad Lightine Cammad Lightine Cammad Lightine Cammad Lightine Cross Cammad Light | | | | | | | | | | | | | | 86.15% |
| Administry Camman lightim | | | | | | | | | | | | | | 100.00% 62.96% |
| Arbitrary Cumman layer (CV-2012-2344) Arbitrary Cumman layer (CV-2012-2374) Arbitrary Cumman layer (CV-2012- | | | | | | | | | | | | | | 88.23% |
| Archivery Cummand lepictum Cummand | | | | | | | | | | | | | | 100.00% |
| Arbitrary Command lighting CWE-2012-2399 **Section CWE-2012-2399 **Se | | | portprocesses‡ | | | | | | | | | | | 88.57% 75.00% |
| Arthursey Command legislates Arthurse Command legislates CW-2012-1407 Arthurse Command legislates CW-2012-1408 Arthurse Command legislates CW-2012-1408 Arthurse Command legislates CW-2012-1408 Arthurse Command legislates CW-2012-1408 Arthurse CW-2012-1409 Arthurse CW-20 | | | ps ps-kill | | | | | | | | | | | 100.00% |
| Arthorny Cammand higherina | Arbitrary Command Injection | CVE-2021-23374 | | 11 | 99 | 11 | 72 | 110 | 0 | 83 | 0 | 29 | 14.79% | 76.68% |
| Anthrage Cummad higheston Anthrage Cummad higheston Anthrage Cummad higheston Cummand higheston Cummand higheston Cummand higheston Cummand higheston Cummand higheston CVF-201-14642 Gummand highest | | CVE-2021-23380 | | | | | | | | | | | | 70.81% |
| Architery Command liquident (VE-2018-3772) Architery Command liquident (VE-2018-2009) Command liquident (V | | l ', | _ | | | | | | | | | | | 56.52% 87.50% |
| Command hybrid | | CVE-2018-3772 | | | | | | | | | | | | 83.33% |
| Command Injection CVE-2020-7616 Figure 1 1 99 11 73 110 87 13 33 33 79 2329 2 | | | | | | | | | | | | | | 76.92% |
| Command Epicelian CVE-2013-1403 affred-wordshownodely 10 93 4 70 10 10 17 10 10 | | | | | | | | | | | | | | 92.85% 91.30% |
| Commund Injection CVE-203-763 apre-publish statistics 10 95 9 73 103 0 82 0 8 7.796 | | CVE-2020-7030 | | 1 | | | | | | | | | | 86.95% |
| Commond Injection CVE-203-7518 Section 11 99 11 72 110 0 53 0 0.0428 | Command Injection | | apex-publish-static-files | 10 | 95 | 9 | 73 | 105 | 0 | 82 | 0 | 8 | 7.76% | 7.76% |
| Commond Rejection CVE-2009-7700 Nestrip: 11 99 11 82 110 87 92 35 4,204 12,007 | Command Injection | | apiconnect-cli-plugins; | | | | | | | | | | 8.83% | 11.43% |
| Communal fajection CVE-2039-7987 Mameri 10 93 3 57 103 0 60 0 1,655 13.88 | | | | | | | | | | | | | | 74.19% 89.04% |
| Command Injection CVE-2020-7915 cd-messeager 10 95 9 72 105 0 81 0 374 3577 34 2,075 34 34 34 34 34 34 34 3 | | | | 1 | | | | | | | | | | 89.04% 57.57% |
| Command Injection | Command Injection | CVE-2020-7795 | | 10 | 95 | 9 | 72 | 105 | 0 | 81 | 0 | 374 | 36.77% | 83.33% |
| Command Injection CV-2309-15123 codecory 10 55 7 76 103 87 81 377 1.985 8.5.95 | Command Injection | CVE-2020-7613 | clamscan; | | | | | | | | | | 8.16% | 21.28% |
| Command Injection CVE-2029-7615 companies-compile 10 93 3 77 103 0 60 0 202 13.966 Command Injection CVE-2029-7815 companies-contected 10 95 9 72 110 0 83 0 73 60.978 Command Injection CVE-2029-28425 cort s 11 99 11 72 110 0 83 0 73 60.978 Command Injection CVE-2029-28425 cort s 11 99 11 72 110 0 83 0 73 60.978 Command Injection CVE-2029-28425 cort s 11 99 11 72 110 0 83 0 73 9.937 Command Injection CVE-2029-7616 Command Injection CVE-2029-2762 Command Injection CVE-2029-7624 Command Injection | | CVF-2020-15123 | | | | | | | | | | | | 9.17% 8.53% |
| Command Injection CVE-2020-781RJB connection-tester 10 95 9 72 105 0 81 0 43 68-256 Command Injection CVE-2020-26188 configure 11 99 11 72 110 0 83 0 1339 99/38 Command Injection CVE-2020-26188 disference 11 99 11 72 110 0 83 0 1339 99/38 Command Injection CVE-2020-2618 disference 11 99 11 72 110 0 83 0 1339 99/38 Command Injection CVE-2020-2618 disference 11 99 11 72 110 0 83 0 23 1519 1519 Command Injection CVE-2020-2618 disference 11 99 11 72 110 0 83 0 23 1519 1519 COmmand Injection CVE-2020-2618 disference 11 99 11 72 110 0 83 0 23 1519 1519 COmmand Injection CVE-2020-2618 Command Injection CVE-2020-2619 COmmand | | | | | | | | | | | | | | 95.65% |
| Commund Injection CVE-200-2442 couries 11 99 11 77 110 0 83 0 75 66.37% | Command Injection | CVE-2020-7781TAB | connection-tester | | 95 | 9 | 72 | | 0 | | | 43 | | 67.74% |
| Command Injection | | | | | | | | | | | | | | 85.24% |
| Command Injection | | | | | | | | | | | | | | 78.12% 87.75% |
| Command Injection | | / | | | | | | | | | | | | 94.82% |
| Command Injection Command Inje | | | | 1 | | | | | | | | | | 32.39% |
| Command higecism Comman | | | | 1 | | | | | | | | | | 88.88% |
| Command Injection | | | | 1 | | | | | | | | | | 87.80% 66.66% |
| Command Injection | | | | 1 | | | | | | | | | | 36.95% |
| Command Injection CVE-2029-38429 Freespace 11 101 11 80 112 0 91 0 27 44.26% | | CVE-2021-23376 | ffmpeg-sdk ‡ | 1 | | | | | | | | | | 75.00% |
| Command Injection CVE-2023-3449 Command Injection CVE-2023-340 global create 11 101 11 88 112 0 91 0 13 65 50 65 60 65 65 | | /, | | | | | | | | | | | | 42.96% |
| Command Injection CVE-2020-8644 gib-ade-remote 11 101 11 80 112 0 91 0 13 65.00% Command Injection CVE-2018-3785 gib-dumny-command 11 101 11 87 110 0 83 0 9 15.00% Command Injection CVE-2018-3786 gib-dumny-command 11 101 11 87 110 0 83 0 9 15.00% Command Injection CVE-2018-3786 gib-dumny-command 11 101 11 87 110 0 83 0 9 15.00% Command Injection CVE-2018-3866 gib-dumny-commands 10 93 9 11 72 110 0 83 0 22.66 32.14% Growth | | CVE-2020-28429 | | | | | | | | | | | | 59.09% 100.00% |
| Command Injection CVE-2018-3785 gil-dummy-commit 11 101 11 87 112 0 98 0 490 7,41% | | | | | | | 80 | | | | | | 65.00% | 65.00% |
| Command Injection CVE-2019-10802 giting 11 99 11 73 110 87 83 34 197 2002% Command Injection / | | | | | | | | | | | | | | 75.00% |
| Command Injection CVE-202-1440 git-interface 10 93 9 60 103 0 69 0 94 68.11% Command Injection CVE-201-16042 growt 10 93 3 57 103 0 60 0 13 52.00% Command Injection CVE-201-16042 growt 10 93 3 57 103 0 60 0 13 52.00% Command Injection CVE-201-36659 gry 11 99 11 74 110 87 83 34 190 59.00% Command Injection CVE-201-201 gulp-ses-lint; 11 99 11 74 110 87 83 34 190 59.00% Command Injection CVE-2020-7601 gulp-ses-lint; 11 99 11 86 110 87 91 44 664 1.30% Command Injection CVE-2020-7605 gulp-tape 11 99 11 86 110 87 91 44 52 50%% Command Injection CVE-2020-2817 heroda-care 11 99 11 86 110 87 91 44 32 50%% Command Injection CVE-2020-2817 heroda-care 11 99 11 86 110 87 91 44 32 50%% Command Injection CVE-2020-2817 heroda-care 11 99 11 72 110 0 83 0 42 93.33% Command Injection CVE-2021-2818 killing: 11 99 11 72 110 0 83 0 42 93.33% Command Injection CVE-2021-2818 killing: 11 99 11 72 110 0 83 0 38 97%% Command Injection CVE-2018-1666 killing: 11 99 11 72 110 0 83 0 38 97%% Command Injection CVE-2018-1666 killing: 11 99 11 72 110 0 83 0 38 97%% Command Injection CVE-2018-1666 killing: 11 99 11 72 110 0 83 0 38 97%% Command Injection CVE-2018-1666 killing: 11 99 11 72 110 0 83 0 54 91.30% Command Injection CVE-2018-1666 killing: 11 99 11 72 110 0 83 0 54 91.30% Command Injection CVE-2019-10783 bof command Injection CVE-2019-10783 bof command Injection CVE-2019-10783 bof command Injection CVE-2020-2844 monoropo-build 10 95 7 72 10 0 83 0 93 73 73 73 73 73 73 73 | | | | | | | | | | | | | | 88.88% 64.56% |
| Command Injection CVE-202-28436 google-countstorage-commands 10 93 3 57 103 0 60 0 13 52.0% | | | | | | | | | | | | | | 68.11% |
| Command Injection CVE-2030-5669 Command Injection CVE-2030-5670 Command Injection CVE-2030-5672 Command Injection CVE-2030-5629 Injection CVE-2030-5630 Injection CVE-2030-5631 Injection CVE-2030-56 | | / | | | | | | | | | | | | 100.00% |
| Command Injection CVE-2029-7661 gry 11 99 11 74 110 87 83 34 190 59.00% Command Injection CVE-2029-7661 gulp-ses-init 11 99 11 86 110 87 87 91 44 664 1.30% Command Injection CVE-2029-7665 gulp-dape 11 99 11 86 110 87 91 44 664 1.30% Command Injection CVE-2029-7685 Gulp-dape 11 99 11 75 110 87 85 34 25 33.33% Command Injection CVE-2019-10788 im-resize 10 93 3 57 103 0 60 0 85 196.3% Command Injection CVE-2019-10787 im-resize 10 93 3 57 103 0 60 0 85 196.3% Command Injection CVE-2019-1629 islone 10 93 3 57 103 0 60 0 1.916 90.1% Command Injection CVE-2019-1649 kill-port-process 11 101 11 81 112 87 91 33 259 20.45% Command Injection CVE-2019-1649 kill-port-process 11 101 11 81 112 87 91 33 259 20.45% Command Injection CVE-2019-1649 kill-port-process 11 101 11 81 112 87 91 33 259 20.45% Command Injection CVE-2019-1649 kill-port-process 11 101 11 81 112 87 91 33 259 20.45% Command Injection CVE-2019-1678 kord 11 99 11 72 110 0 83 0 54 91.00% Command Injection CVE-2019-1678 kord | | | | | | | | | | | | | | 52.00% |
| Command Injection CVE-2020-7607 gulp-syse-lint; 11 99 9 86 110 87 89 42 5,065 5,065 Command Injection CVE-2020-7605 gulp-style-docco 11 99 11 86 110 87 91 44 664 1.30% 600 | | | _ | | | | | | | | | | | 45.45% 88.23% |
| Command Injection CVE-2020-26437 heroks-env 11 99 11 75 110 87 91 44 32 5.08% | | | | | | | | | | | | | | 40.54% |
| Command Injection CVE-2019-10788 im-metadata 11 99 11 75 110 87 85 34 25 33.33% Command Injection CVE-2019-10787 im-resize 10 93 3 57 103 0 60 0 85 19.63% Command Injection CVE-2020-7629 install-package 11 99 11 72 110 0 83 0 42 03.33% Command Injection CVE-2019-1878 jison 10 93 3 57 103 0 60 0 0 1.916 9.01% Command Injection CVE-2012-1388 illing 11 99 11 72 110 0 83 0 36 9.05% Command Injection CVE-2019-15699 illinomap 11 99 11 74 110 87 83 34 25 33.33% Command Injection CVE-2019-15699 illinomap 11 99 11 74 110 87 83 34 3.069 6.30% Command Injection CVE-2019-15690 illinomap 11 99 11 74 110 87 83 34 3.069 6.30% Command Injection CVE-2019-1864 illinomap 11 99 11 72 110 0 83 0 54 91.30% Command Injection CVE-2019-1866 illinomap 11 99 11 72 110 0 83 0 54 91.30% Command Injection CVE-2019-1866 macromip 11 99 11 72 110 0 83 0 54 91.30% COMMAND Injection CVE-2019-1866 macromip 11 99 11 75 110 87 85 34 39 45.85% Command Injection CVE-2019-1866 macromip 11 99 11 75 110 87 85 34 39 45.85% Command Injection CVE-2019-1866 macromip 11 99 11 72 110 0 83 0 93 45.85% Command Injection CVE-2019-1866 macromip 11 99 11 72 110 0 83 0 93 77.50% Command Injection CVE-2019-1867 mode-lexe-sender 11 99 11 72 110 0 83 0 94 94.85% Command Injection CVE-2019-1863 mode-lexe-sender 11 99 11 72 110 0 83 0 95 77.50% Command Injection CVE-2019-1864 mode-prop-base 11 99 11 72 110 0 83 0 95 77.50% Command Injection CVE-2019-602 mode-sender 11 99 11 72 110 0 83 0 96 97.50% Command Injection CVE-2019-602 mode-sender 11 99 11 72 110 0 83 0 | | | | | | | | | | | | | | 77.08% |
| Command Injection | | | | | | | | | | | | | | 84.21% 42.00% |
| Command Injection CVE-2019-10787 install-package; 10 93 3 57 103 0 60 0 85 19.63% Command Injection CVE-2020-8418 jison 10 93 3 57 103 0 60 0 1.916 93.34 Command Injection CVE-2019-15609 kill-port-process 11 101 11 81 112 87 91 33 259 20.45% Command Injection CVE-2019-15609 kill-port-process 11 101 11 81 112 87 91 33 259 20.45% Command Injection CVE-2019-15609 kill-port-process 11 101 11 81 112 87 91 33 259 20.45% Command Injection CVE-2019-15609 kill-port-process 10 93 8 79 103 87 66 57 37 37.37% Command Injection CVE-2019-16780 sof 11 99 11 72 110 0 83 0 54 19.30% Command Injection CVE-2019-16780 kill-port-process 11 101 11 81 112 87 91 33 259 20.45% Command Injection CVE-2019-16780 kof 11 99 11 72 110 0 83 0 54 19.30% Command Injection CVE-2019-16786 monorepo-build 10 93 4 61 103 87 63 35 17.715 34.02% Command Injection CVE-2019-16786 monorepo-build 10 95 7 7 72 105 0 79 0 78.10 78.810 78.88% Command Injection CVE-2019-15897 mode-key-sendert; 11 99 11 72 110 0 83 0 93 88.47% Command Injection CVE-2020-2643 mode-key-sendert; 11 99 11 72 110 0 83 0 93 77.50% Command Injection CVE-2020-3622 mode-key-sendert; 11 99 11 72 110 0 83 0 93 77.50% Command Injection CVE-2020-3623 mode-mpv 10 95 7 72 105 0 79 0 36 14.63% Command Injection CVE-2020-7682 mode-mpv 10 95 7 72 105 0 79 0 36 14.63% Command Injection CVE-2020-7684 mode-prop-here 10 95 7 72 105 0 79 0 36 14.63% Command Injection CVE-2020-7682 mode-mpv 10 95 7 72 105 0 79 0 36 6.66% Command Injection CVE-2020-7684 pand-injection CVE-2020-7684 pand-in | | | | | | | | | | | | | | 83.72% |
| Command Injection CVE-2020-8178 jison 10 93 3 57 103 0 60 0 1,916 9,01% | | CVE-2019-10787 | im-resize | | 93 | 3 | 57 | 103 | 0 | | 0 | | 19.63% | 85.71% |
| Command Injection CVE-2019-15609 Kill-port-process 11 99 11 72 110 0 83 0 38 9.76% | | | | | | | | | | | | | | 93.33% |
| Command Injection CVE-2019-1609 kill-port-process 11 101 11 81 112 87 91 33 259 20.45% Command Injection CVE-2018-16461 lihmnap 11 99 11 74 110 87 83 34 3,069 20.45% Command Injection CVE-2019-10783 CVE-2019-10783 CVE-2019-10783 CVE-2019-10783 CVE-2019-10786 Injury of the command Injection CVE-2020-2786 Injury of the command Injection CVE-2020-2786 Injury of the command Injection CVE-2020-28414 Injury of the command Injection CVE-2019-10786 Injury of the command Injection CVE-2019-15786 Injury of the command Injection CVE-2019-15785 Injury of the command Injection CVE-2019-1785 Injury of the command Injection CVE-2019-1785 Injury of the command Injection CVE-2019-1796 Inju | | | | | | | | | | | | | | 61.24% 90.24% |
| Command Injection CVE-2019-10783 sof 11 99 11 72 110 0 83 0 54 91.30% | Command Injection | CVE-2019-15609 | kill-port-process | 11 | 101 | 11 | 81 | 112 | 87 | 91 | 33 | 259 | 20.45% | 56.75% |
| Command Injection CVE-2019-10783 Isof 11 99 11 72 110 0 83 0 54 91.30% | | CVE-2018-16461 | | | | | | | | | | | | 80.93% |
| Command Injection CVE-2020-786 macfromip 11 99 11 75 110 87 85 34 39 45.88% Command Injection CVE-2020-28434 monorepo-build 10 95 7 72 105 0 79 0 7.810 7.58% Command Injection CVE-2019-1686 metwork-manager 10 95 9 72 105 0 81 0 93 89.42% Command Injection CVE-2020-7627 mode-def 11 99 11 72 110 0 83 0 93 89.42% Command Injection CVE-2020-7627 mode-latex-pdf 11 99 11 72 110 0 83 0 93 77.50% Command Injection CVE-2020-7632 mode-mpv 10 95 7 72 105 0 79 0 36 14.63% Command Injection CVE-2020-7632 mode-mpv 10 95 7 72 105 0 79 0 8 6.66% CVE-2020-785 mode-prompt-here 10 95 7 72 110 0 83 0 97 0 36 14.63% Command Injection CVE-2020-785 mode-prompt-here 10 95 7 72 110 0 83 0 37 75.51% Command Injection CVE-2020-785 mode-unrar 11 99 11 72 110 0 83 0 37 75.51% Command Injection CVE-2021-23375 mode-unrar 11 99 11 72 110 0 83 0 37 75.51% Command Injection CVE-2021-2403 mode-unrar 11 99 11 72 110 0 83 0 37 75.51% Command Injection CVE-2021-2403 mode-unrar 11 99 11 72 110 0 83 0 63 61.2% Command Injection CVE-2021-2403 react-dev-utils 10 95 9 72 105 0 81 0 64.25 17.7% Command Injection CVE-201-2403 react-dev-utils 10 95 9 72 105 0 81 0 64.25 64.24 82.9% Command Injection CVE-201-2043 react-dev-utils 10 95 9 72 105 0 81 0 64.25 64.24 82.9% Command Injection CVE-2020-7624 strong-nginx-controller 10 93 4 58 103 87 60 33 1.721 1.75 | | CVE-2010 10782 | | | | | | | | | | | | 55.73% 91.30% |
| Command Injection CVE-2020-786 macfromip 11 99 11 75 110 87 85 34 39 45.88% Command Injection CVE-2019-10786 metwork-manager 10 95 7 72 105 0 81 0 93 89.42% Command Injection CVE-2019-10786 metwork-manager 10 95 9 72 105 0 81 0 93 89.42% Command Injection CVE-2019-1627 node-df 11 99 11 72 110 0 83 0 84 1.71% Command Injection CVE-2020-2843 node-latex-pdf 11 99 11 72 110 0 83 0 93 75.50% Command Injection CVE-2020-3843 node-latex-pdf 11 99 11 72 110 0 83 0 9 60.00% Command Injection CVE-2020-7632 node-prompt-here 10 95 7 72 105 0 79 0 36 14.63% Command Injection CVE-2020-7785 node-prompt-here 10 95 7 72 105 0 79 0 8 6.66% Command Injection CVE-2020-788 node-prompt-here 10 95 7 72 110 0 83 0 37 75.51% Command Injection CVE-2021-33375 node-unrar 11 99 11 72 110 0 83 0 37 75.51% Command Injection CVE-2021-604 pulverizr 11 99 11 72 110 0 83 0 63 70.1% Command Injection CVE-2019-1096 psinode 11 99 11 72 110 0 83 0 63 70.1% Command Injection CVE-2019-1096 psinode 11 99 11 72 110 0 83 0 63 70.1% Command Injection CVE-2019-1096 psinode 11 99 11 77 110 87 87 33 614 6.56% Command Injection CVE-2019-1096 psinode 11 99 11 73 110 87 87 33 642 642.82% Command Injection CVE-2019-1096 psinode 11 99 11 73 110 87 83 33 45 57.69% Command Injection CVE-2019-0804 serial-number 11 99 11 73 110 87 83 33 1.721 15.46% Command Injection CVE-2020-7628 trong-nginx-controller 10 93 4 58 58.29% Command Injection CVE-2020-7628 trong-nginx-controller 10 93 4 58 58.29% Command Injection CVE-2020-7628 trong-nginx-controller 10 93 4 58 58.29% Command Injection C | | / | | | | | | | | | | | | 63.54% |
| Command Injection CVE-2019-10786 network-manager 10 95 9 72 105 0 81 0 93 89.42% | Command Injection | | macfromip | 11 | 99 | 11 | 75 | 110 | 87 | 85 | 34 | 39 | 45.88% | 45.88% |
| Command Injection CVE-2019-15597 node-def 11 99 11 72 110 0 83 0 94 17.50% | | | | | | | | | | | | | | 85.18% |
| Command Injection CVE-2020-7627 node-latex-pdf 11 99 11 72 110 0 83 0 93 77.50% | | | | | | | | | | | | | | 93.00% 91.30% |
| Command Injection CVE-2020-28433 node-lates-pdf 11 99 11 72 110 0 83 0 9 60.00% | | | | | | | | | | | | | | 77.50% |
| Command Injection CVE-2020-7602 node-prompi-here 10 95 7 72 105 0 79 0 8 6.66% | Command Injection | | node-latex-pdf | 11 | 99 | 11 | 72 | 110 | 0 | 83 | | 9 | 60.00% | 60.00% |
| Command Injection CVE-2020-7785 node-ps 11 99 11 72 110 0 83 0 37 75.51% | | | | | | | | | | | | | | 14.63% |
| Command Injection CVE-2021-841 npm-lockfile\$ 10 93 3 57 103 0 60 0 1,963 7.01% | | | | | | | | | | | | | | 57.14% 75.51% |
| Command Injection CVE-2022-33375 npm-lockfile 10 93 3 57 103 0 66 0 0 1,963 7,01% | | | | | | | | | | | | | | 100.00% |
| Command Injection CVE-2020-7604 pulverizr 11 99 11 77 110 87 87 33 614 6.56% CVE-2021-24033 react-dev-utils 10 95 9 72 105 0 81 0 6.425 11.77% Command Injection CVE-2019-10796 rpi 11 99 11 72 110 0 83 0 28 65.11% Command Injection CVE-2019-10804 serial-number 11 99 11 73 110 87 83 33 45 57.69% Command Injection CVE-2020-7621 strong-nginx-controller 10 93 3 57 103 0 60 0 17.994 6.37% Command Injection CVE-2020-38432 theme-core‡ 10 93 4 58 103 87 60 33 1.721 15.46% Command Injection CVE-2020-7628 umount 11 99 11 73 110 87 83 33 2.376 16.29% Command Injection CVE-2020-7628 umount 11 99 11 75 110 0 83 0 965 8.20% Command Injection VE-2020-7628 umount 11 99 11 75 110 87 85 34 55 58.29% Command Injection VE-2020-7628 umount 11 99 11 75 110 87 85 34 55 58.29% Command Injection VE-2020-7628 Umount 11 99 11 75 110 87 85 34 55 58.29% Command Injection VE-2020-7628 Umount 11 99 11 75 110 87 85 34 55 58.29% Command Injection VE-2020-7628 Umount 11 99 11 75 110 87 85 34 55 58.29% Command Injection VE-2020-7628 Umount 11 99 11 75 110 87 85 34 55 58.29% Command Injection VE-2020-7628 Umount | | | npm-lockfile; | 10 | 93 | 3 | 57 | 103 | 0 | 60 | | 1,963 | 7.01% | 70.96% |
| Command Injection CVE-2021-24033 react-dev-utils 10 95 9 72 105 0 81 0 6,425 11.77% | | | | | | | | | | | | | | 35.13% |
| Command Injection CVE-2019-10796 rpi 11 99 11 72 110 0 83 0 28 65.11% | | | | | | | | | | | | | | 87.02% 22.32% |
| Command Injection CVE-2019-10804 serial-number 11 99 11 73 110 87 83 33 45 57.69% | | | | | | | 72 | | 0 | | | | | 65.00% |
| Command Injection CVE-2020-7621 strong-nginx-controller 10 93 3 57 103 0 60 0 17,994 6.37% Command Injection CVE-2020-28432 theme-core\$\(^{\frac{1}{2}}\) 10 93 4 58 103 87 60 33 1.721 15.46% Command Injection CVE-2020-7784 ts-process-promises 11 99 11 73 110 87 83 33 2.376 16.29% Command Injection CVE-2020-7628 umount 11 99 11 75 110 0 83 0 965 8.20% Command Injection 7 vboxmanage_j\$\(^{\frac{1}{2}}\) 11 99 11 75 110 87 85 34 55 52.82% 18 18 18 18 18 18 18 1 | Command Injection | CVE-2019-10804 | serial-number | | | | | | | | | | 57.69% | 57.69% |
| Command Injection CVE-2020-28432 theme-core: 10 93 4 58 103 87 60 33 1,721 15.46% Command Injection CVE-2020-7784 ts-process-promises 11 99 11 73 110 87 83 33 2,376 16.29% Command Injection CVE-2020-7628 umount 11 99 11 72 110 0 83 0 965 8.20% Command Injection / vboxmanage.js; 11 99 11 75 110 87 85 34 55 25.82% | | | | | | | | | | | | | | 42.40% |
| Command Injection CVE-2020-7784 ts-process-promises 11 99 11 73 110 87 83 33 2,376 16.29% Command Injection CVE-2020-7628 umount 11 99 11 72 110 0 83 0 965 8.20% Command Injection / vboxmanage,js² 11 99 11 75 110 87 85 34 55 25.82% | | | | | | | | | | | | | | 49.70% 81.35% |
| Command Injection CVE-2020-7628 umount 11 99 11 72 110 0 83 0 965 8.20% Command Injection / vboxmanage is* 11 99 11 75 110 87 85 34 55 25.82% | | | | | | | 73 | | | | | | | 84.76%% |
| | Command Injection | | umount | | | | | | | | 0 | 965 | 8.20% | 71.73% |
| | | | | | | | | | | | | | | 25.82% |
| Command Injection CVE-2020-15362 wifescanner 11 99 11 73 110 0 83 0 31 0.44% Command Injection CVE-2020-15362 wifescanner 11 99 11 73 110 87 83 33 215 9.10% | Command Injection Command Injection | CVE-2020-28431 CVE-2020-15362 | wc-cmd‡ wifiscanner | 11 | 99 99 | 11 | 72 73 | 110 110 | 0 87 | 83 83 | 0 33 | 31 215 | 0.44% 9.10% | 82.50% 83.33% |

| Commond Injection | CVE-2020-28447 | l | l 11 | 99 | l 11 | 72 | 110 | 1 0 | 83 | 1 0 | 1 9 | 90.00% | 90.00% |
|--|---------------------------------------|---------------------------------------|-------|----------|------|----------|----------|-------|----------|-------|--------------|------------------|--|
| Command Injection Command Injection | CVE-2020-28447 | xopen‡ xps | 11 | 99 | 11 | 72 | 110 | 0 | 83 | 0 | 51 | 4.26% | 90.00% 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 kmc | 6 | 28 83 | 1 | 28 45 | 29 89 | 0 | 29 46 | 0 | 397 2,267 | 74.62% 6.02% | 74.62% 55.81% |
| Arbitrary Code Injection | l ', | marsdb | 0 | 28 | 1 | 28 | 29 | 0 | 29 | 0 | 1,825 | 18.20% | 54.06% |
| Arbitrary Code Injection Arbitrary Code Injection | l ', | mixin-pro | 1 | 28 | 1 | 28 | 29 | 0 | 29 | 0 | 78 | 82.10% | 82.10% |
| Arbitrary Code Injection | l ', | m-log | 1 | 28 | l i | 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 | , | 1 | 1 |
| Arbitrary Code Injection | , , , , , , , , , , , , , , , , , , , | modis | 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 28 | 1 1 | 28 28 | 29 29 | 0 | 29 29 | 0 | 81 | 0.26% | 96.42% |
| Code Injection | CVE-2021-21277 CVE-2020-7675 | angular-expressions | 1 1 | 28 | 1 1 | 28 | 29 | 0 | 29 | 0 | 713 374 | 48.01% 36.77% | 48.01% 90.69% |
| Code Injection Code Injection | CVE-2018-3784 | cd-messenger | 1 | 28 | 1 | 28 | 29 | 0 | 29 | 0 | 90 | 84.11% | 84.11% |
| Code Injection | CVE-2019-15657 | cryop 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 | ī | 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 28 | 1 | 38 28 | 89 29 | 0 | 39 29 | 0 | 1,118 | 3.59% 33.44% | 78.18% 55.35% |
| Remote Code Execution Remote Code Execution | l ', | djv | 7 | 90 | 3 | 60 | 97 | 87 | 59 | 35 | 300 2,688 | 5.32% | 28.49% |
| Remote Code Execution | CVE-2019-10758 | mongodb-query-parser 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 | i | 28 | l i | 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 | | | | | <u> </u> | 1 ′ | 1 ' | ' | | ' | 1 | <u>' </u> |
| | Aroitrary 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;
TP: Thread Pool system calls invocation;
TP: Thread Pool system calls invocation;
TP: Packages that invoke system calls that are triggered by the execution of builtin methods;
CL: Covered line of the package;
CL-1: Covered line of the package;
CL-2: Covered line of the package module;