

Clingto / [gist:bb632c0c463f4b2c97e4f65f751c5e6d](https://gist.github.com/Clingto/bb632c0c463f4b2c97e4f65f751c5e6d)

Created 5 months ago

☆ Star

&lt;&gt; Code ↻ Revisions 1

Minimum information for the vulnerability covered by 32 CVEs.

gistfile1.txt

```
1 1. For Memory Leak in mjs ES6 use:
2 CVE-2021-33437
3
4 Suggested Description:
5
6 An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There are memory leaks in frozen_cb() in mjs
7
8 Additional Information:
9 🕒 ● The cveform.mitre.org "VulnerabilityType Other" field was set
10 to: memory leak
11
12 ● The cveform.mitre.org "Affected Component" field was set to:
13 mjs.c, frozen_cb(), mjs.
14
15 ● The cveform.mitre.org "Attack Type" field was set to: Local
16
17 ● The cveform.mitre.org "Impact Denial of Service" field was
18 set to: true
19
20 ● The cveform.mitre.org "Attack Vectors" field was set to: To
21 exploit vulnerability, someone must open a crafted file, like
22 https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-5794-
23 frozen_cb-memory-leak
24
25 ● The cveform.mitre.org "Reference" field was set to:
26 https://github.com/cesanta/mjs/issues/160
27
28 ● The cveform.mitre.org "Vendor of Product" field was set to:
29 https://github.com/cesanta/mjs
30
31 ● The cveform.mitre.org "Affected Product Code Base" field was
32 set to: mjs ES6 (JavaScript version 6)
33
34 ● The cveform.mitre.org "Suggested description" field was set
35 to: An issue was discovered in mjs(mJS: Restricted JavaScript
36 engine), ES6 (JavaScript version 6). There are memory leaks
37 in frozen_cb() in mjs.c.
38
39 🏠 The cveform.mitre.org 1001319 submission was from:
40 cfenicey@gmail.com
41
42 -----
43 2. For Buffer Overflow in mjs ES6 use:
44 CVE-2021-33438
45
46 Suggested Description:
47
48 An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is stack buffer overflow in json_pars
49
50 Additional Information:
51
52 🕒 ● The cveform.mitre.org "Vulnerability Type" field was set to:
53 Buffer Overflow
54
55 ● The cveform.mitre.org "Affected Component" field was set to:
56 mjs.c, json_parse_array(), mjs.
57
58 ● The cveform.mitre.org "Attack Type" field was set to: Local
59
60 ● The cveform.mitre.org "Impact Denial of Service" field was
61 set to: true
62
63 ● The cveform.mitre.org "Attack Vectors" field was set to: To
64 exploit vulnerability, someone must open a crafted file, like
65 https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-5fb78
66 -json_parse_array-stack-overflow
67
68 ● The cveform.mitre.org "Reference" field was set to:
69 https://github.com/cesanta/mjs/issues/158
70
71 ● The cveform.mitre.org "Vendor of Product" field was set to:
72 https://github.com/cesanta/mjs
73
74 ● The cveform.mitre.org "Affected Product Code Base" field was
75 set to: mjs ES6 (JavaScript version 6)
76
77 ● The cveform.mitre.org "Suggested description" field was set
78 to: An issue was discovered in mjs(mJS: Restricted JavaScript
79 engine), ES6 (JavaScript version 6). There is stack buffer
80
```

```
81 | overflow in json_parse_array() in mjs.c.
82 |
83 | 🚩 The cveform.mitre.org 1001319 submission was from:
84 | cfenicey@gmail.com
85 |
86 | -----
87 |
88 | 3. For NULL pointer dereference in mjs ES6 use:
89 |
90 | CVE-2021-33439
91 |
92 | Suggested Description:
93 |
94 | An issue was discovered in mjs(mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in gc_comp
95 |
96 | Additional Information:
97 |
98 | 🚩 ● The cveform.mitre.org "Vulnerability Type" field was set to:
99 | NULL pointer dereference
100 |
101 | ● The cveform.mitre.org "Affected Component" field was set to:
102 | mjs.c, gc_compact_strings(), mjs.
103 |
104 | ● The cveform.mitre.org "Attack Type" field was set to: Local
105 |
106 | ● The cveform.mitre.org "Impact Denial of Service" field was
107 | set to: true
108 |
109 | ● The cveform.mitre.org "Attack Vectors" field was set to: To
110 | exploit vulnerability, someone must open a crafted file, like
111 | https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-8d05d
112 | -gc_compact_strings-negative-size-param
113 |
114 | ● The cveform.mitre.org "Reference" field was set to:
115 | https://github.com/cesanta/mjs/issues/159
116 |
117 | ● The cveform.mitre.org "Vendor of Product" field was set to:
118 | https://github.com/cesanta/mjs
119 |
120 | ● The cveform.mitre.org "Affected Product Code Base" field was
121 | set to: mjs ES6 (JavaScript version 6)
122 |
123 | ● The cveform.mitre.org "Suggested description" field was set
124 | to: An issue was discovered in mjs(mJS: Restricted JavaScript
125 | engine), ES6 (JavaScript version 6). There is Integer
126 | overflow in gc_compact_strings() in mjs.c.
127 |
128 | 🚩 The cveform.mitre.org 1001319 submission was from:
129 | cfenicey@gmail.com
130 | -----
131 |
132 | 4. For NULL pointer dereference in mjs ES6 (github issue 163) use:
133 |
134 | CVE-2021-33440
135 |
136 | Suggested Description:
137 |
138 | An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_bc
139 |
140 | Additional Information:
141 |
142 | 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set
143 | to: NULL pointer dereference
144 |
145 | ● The cveform.mitre.org "Affected Component" field was set to:
146 | mjs.c, mjs_bcode_commit(), mjs.
147 |
148 | ● The cveform.mitre.org "Attack Type" field was set to: Local
149 |
150 | ● The cveform.mitre.org "Impact Denial of Service" field was
151 | set to: true
152 |
153 | ● The cveform.mitre.org "Attack Vectors" field was set to: To
154 | exploit vulnerability, someone must open a crafted file, like
155 | https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-7954-
156 | mjs_bcode_commit-null-pointer-deref
157 |
158 | ● The cveform.mitre.org "Reference" field was set to:
159 | https://github.com/cesanta/mjs/issues/163
160 |
161 | ● The cveform.mitre.org "Vendor of Product" field was set to:
162 | https://github.com/cesanta/mjs
163 |
164 | ● The cveform.mitre.org "Affected Product Code Base" field was
165 | set to: mjs ES6 (JavaScript version 6)
166 |
167 | ● The cveform.mitre.org "Suggested description" field was set
168 | to: An issue was discovered in mjs(mJS: Restricted JavaScript
169 | engine), ES6 (JavaScript version 6). There is NULL pointer
170 | dereference in mjs_bcode_commit() in mjs.c.
171 |
172 | 🚩 The cveform.mitre.org 1001319 submission was from:
173 | cfenicey@gmail.com
174 | -----
175 |
176 | 5. For NULL pointer dereference in mjs ES6 (github issue 165) use:
177 |
178 | CVE-2021-33441
```

```
179
180 Suggested Description:
181
182 An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in exec_e
183
184 Additional Information:
185
186 📌 ● The cveform.mitre.org "VulnerabilityType Other" field was set
187 to: NULL pointer dereference
188
189 ● The cveform.mitre.org "Affected Component" field was set to:
190 mjs.c, exec_expr(), mjs.
191
192 ● The cveform.mitre.org "Attack Type" field was set to: Local
193
194 ● The cveform.mitre.org "Impact Denial of Service" field was
195 set to: true
196
197 ● The cveform.mitre.org "Attack Vectors" field was set to: To
198 exploit vulnerability,someone must open a crafted file,like
199 https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-9035-
200 exec_expr-null-pointer-deref
201
202 ● The cveform.mitre.org "Reference" field was set to:
203 https://github.com/cesanta/mjs/issues/165
204
205 ● The cveform.mitre.org "Vendor of Product" field was set to:
206 https://github.com/cesanta/mjs
207
208 ● The cveform.mitre.org "Affected Product Code Base" field was
209 set to: mjs ES6 (JavaScript version 6)
210
211 ● The cveform.mitre.org "Suggested description" field was set
212 to: An issue was discovered in mjs(mJS: Restricted JavaScript
213 engine), ES6 (JavaScript version 6). There is NULL pointer
214 dereference in exec_expr() in mjs.c.
215
216 📌 The cveform.mitre.org 1001319 submission was from:
217 cfenicey@gmail.com
218 -----
219
220 6. For NULL pointer dereference in mjs ES6 (github issue 161) use:
221
222 CVE-2021-33442
223
224 Suggested Description:
225
226 An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in json_p
227
228 Additional Information:
229
230 📌 ● The cveform.mitre.org "VulnerabilityType Other" field was set
231 to: NULL pointer dereference
232
233 ● The cveform.mitre.org "Affected Component" field was set to:
234 mjs.c, json_printf(), mjs.
235
236 ● The cveform.mitre.org "Attack Type" field was set to: Local
237
238 ● The cveform.mitre.org "Impact Denial of Service" field was
239 set to: true
240
241 ● The cveform.mitre.org "Attack Vectors" field was set to: To
242 exploit vulnerability,someone must open a crafted file,like
243 https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-6368-
244 json_printf-null-pointer-deref
245
246 ● The cveform.mitre.org "Reference" field was set to:
247 https://github.com/cesanta/mjs/issues/161
248
249 ● The cveform.mitre.org "Vendor of Product" field was set to:
250 https://github.com/cesanta/mjs
251
252 ● The cveform.mitre.org "Affected Product Code Base" field was
253 set to: mjs ES6 (JavaScript version 6)
254
255 ● The cveform.mitre.org "Suggested description" field was set
256 to: An issue was discovered in mjs(mJS: Restricted JavaScript
257 engine), ES6 (JavaScript version 6). There is NULL pointer
258 dereference in json_printf() in mjs.c.
259
260 📌 The cveform.mitre.org 1001319 submission was from:
261 cfenicey@gmail.com
262 -----
263
264 7. For NULL pointer dereference in mjs ES6 (github issue 167) use:
265
266 CVE-2021-33443
267
268 Suggested Description:
269
270 An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is stack buffer overflow in mjs_execu
271
272 Additional Information:
273
274 📌 ● The cveform.mitre.org "VulnerabilityType Other" field was set
275 to: NULL pointer dereference
276
```

```
277 ● The cveform.mitre.org "Affected Component" field was set to:
278 mjs.c, mjs_execute(), mjs.
279
280 ● The cveform.mitre.org "Attack Type" field was set to: Local
281
282 ● The cveform.mitre.org "Impact Denial of Service" field was
283 set to: true
284
285 ● The cveform.mitre.org "Attack Vectors" field was set to: To
286 exploit vulnerability, someone must open a crafted file, like
287 https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-9522-
288 mjs_execute-stack-overflow
289
290 ● The cveform.mitre.org "Reference" field was set to:
291 https://github.com/cesanta/mjs/issues/167
292
293 ● The cveform.mitre.org "Vendor of Product" field was set to:
294 https://github.com/cesanta/mjs
295
296 ● The cveform.mitre.org "Affected Product Code Base" field was
297 set to: mjs ES6 (JavaScript version 6)
298
299 ● The cveform.mitre.org "Suggested description" field was set
300 to: An issue was discovered in mjs(mJS: Restricted JavaScript
301 engine), ES6 (JavaScript version 6). There is stack buffer
302 overflow in mjs_execute() in mjs.c.
303
304 🚩 The cveform.mitre.org 1001319 submission was from:
305 cfenicey@gmail.com
306 -----
307
308 8. For NULL pointer dereference in mjs ES6 (github issue 166) use:
309
310 CVE-2021-33444
311
312 Suggested Description:
313
314 An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in getprop
315
316 Additional Information:
317
318 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set
319 to: NULL pointer dereference
320
321 ● The cveform.mitre.org "Affected Component" field was set to:
322 mjs.c, getprop_builtin_foreign(), mjs.
323
324 ● The cveform.mitre.org "Attack Type" field was set to: Local
325
326 ● The cveform.mitre.org "Impact Denial of Service" field was
327 set to: true
328
329 ● The cveform.mitre.org "Attack Vectors" field was set to: To
330 exploit vulnerability, someone must open a crafted file, like
331 https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-9187-
332 getprop_builtin_foreign-null-pointer-deref
333
334 ● The cveform.mitre.org "Reference" field was set to:
335 https://github.com/cesanta/mjs/issues/166
336
337 ● The cveform.mitre.org "Vendor of Product" field was set to:
338 https://github.com/cesanta/mjs
339
340 ● The cveform.mitre.org "Affected Product Code Base" field was
341 set to: mjs ES6 (JavaScript version 6)
342
343 ● The cveform.mitre.org "Suggested description" field was set
344 to: An issue was discovered in mjs(mJS: Restricted JavaScript
345 engine), ES6 (JavaScript version 6). There is NULL pointer
346 dereference in getprop_builtin_foreign() in mjs.c.
347
348 🚩 The cveform.mitre.org 1001319 submission was from:
349 cfenicey@gmail.com
350 -----
351
352 9. For NULL pointer dereference in mjs ES6 (github issue 169) use:
353
354 CVE-2021-33445
355
356 Suggested Description:
357
358 An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_st
359
360 Additional Information:
361
362 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set
363 to: NULL pointer dereference
364
365 ● The cveform.mitre.org "Affected Component" field was set to:
366 mjs.c, mjs_string_char_code_at(), mjs.
367
368 ● The cveform.mitre.org "Attack Type" field was set to: Local
369
370 ● The cveform.mitre.org "Impact Denial of Service" field was
371 set to: true
372
373 ● The cveform.mitre.org "Attack Vectors" field was set to: To
374 exploit vulnerability, someone must open a crafted file, like
```

```
375 https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-13891
376 -mjs_string_char_code_at-null-pointer-deref
377
378 ● The cveform.mitre.org "Reference" field was set to:
379 https://github.com/cesanta/mjs/issues/169
380
381 ● The cveform.mitre.org "Vendor of Product" field was set to:
382 https://github.com/cesanta/mjs
383
384 ● The cveform.mitre.org "Affected Product Code Base" field was
385 set to: mjs ES6 (JavaScript version 6)
386
387 ● The cveform.mitre.org "Suggested description" field was set
388 to: An issue was discovered in mjs(mJS: Restricted JavaScript
389 engine), ES6 (JavaScript version 6). There is NULL pointer
390 dereference in mjs_string_char_code_at() in mjs.c.
391
392 🚩 The cveform.mitre.org 1001319 submission was from:
393 cfenicey@gmail.com
394 -----
395 10, For NULL pointer dereference in mjs ES6 (github issue 168) use:
396
397 CVE-2021-33446
398
399 Suggested Description:
400
401 An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_ne
402
403 Additional Information:
404
405 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set
406 to: NULL pointer dereference
407
408 ● The cveform.mitre.org "Affected Component" field was set to:
409 mjs.c, mjs_next(), mjs.
410
411 ● The cveform.mitre.org "Attack Type" field was set to: Local
412
413 ● The cveform.mitre.org "Impact Denial of Service" field was
414 set to: true
415
416 ● The cveform.mitre.org "Attack Vectors" field was set to: To
417 exploit vulnerability, someone must open a crafted file, like
418 https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-12318
419 -mjs_next-null-pointer-deref
420
421 ● The cveform.mitre.org "Reference" field was set to:
422 https://github.com/cesanta/mjs/issues/168
423
424 ● The cveform.mitre.org "Vendor of Product" field was set to:
425 https://github.com/cesanta/mjs
426
427 ● The cveform.mitre.org "Affected Product Code Base" field was
428 set to: mjs ES6 (JavaScript version 6)
429
430 ● The cveform.mitre.org "Suggested description" field was set
431 to: An issue was discovered in mjs(mJS: Restricted JavaScript
432 engine), ES6 (JavaScript version 6). There is NULL pointer
433 dereference in mjs_next() in mjs.c.
434
435 🚩 The cveform.mitre.org 1001319 submission was from:
436 cfenicey@gmail.com
437 -----
438 11, For NULL pointer dereference in mjs ES6 (github issue 164) use:
439
440 CVE-2021-33447
441
442 Suggested Description:
443
444 An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_pr
445
446 Additional Information:
447
448 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set
449 to: NULL pointer dereference
450
451 ● The cveform.mitre.org "Affected Component" field was set to:
452 mjs.c, mjs_print(), mjs.
453
454 ● The cveform.mitre.org "Attack Type" field was set to: Local
455
456 ● The cveform.mitre.org "Impact Denial of Service" field was
457 set to: true
458
459 ● The cveform.mitre.org "Attack Vectors" field was set to: To
460 exploit vulnerability, someone must open a crafted file, like
461 https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-7992-
462 mjs_print-null-pointer-deref
463
464 ● The cveform.mitre.org "Reference" field was set to:
465 https://github.com/cesanta/mjs/issues/164
466
467 ● The cveform.mitre.org "Vendor of Product" field was set to:
468 https://github.com/cesanta/mjs
469
470 ● The cveform.mitre.org "Affected Product Code Base" field was
471 set to: mjs ES6 (JavaScript version 6)
472
```

```
473 ● The cveform.mitre.org "Suggested description" field was set
474 to: An issue was discovered in mjs(mJS: Restricted JavaScript
475 engine), ES6 (JavaScript version 6). There is NULL pointer
476 dereference in mjs_print() in mjs.c.
477
478 🚩 The cveform.mitre.org 1001319 submission was from:
479 cfenicey@gmail.com
480 -----
481 12, For Buffer Overflow in mjs ES6 (github issue 170) use:
482
483 CVE-2021-33448
484
485 Suggested Description:
486
487 An issue was discovered in mjs(mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is stack buffer overflow at 0x7ffe904
488
489 Additional Information:
490
491 🚩 ● The cveform.mitre.org "Vulnerability Type" field was set to:
492 Buffer Overflow
493
494 ● The cveform.mitre.org "Affected Component" field was set to:
495 <unknown module>, at 0x7ffe9049390, mjs.
496
497 ● The cveform.mitre.org "Attack Type" field was set to: Local
498
499 ● The cveform.mitre.org "Impact Denial of Service" field was
500 set to: true
501
502 ● The cveform.mitre.org "Attack Vectors" field was set to: To
503 exploit vulnerability, someone must open a crafted file, like
504 https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-module-stack-overflow
505
506 ● The cveform.mitre.org "Reference" field was set to:
507 https://github.com/cesanta/mjs/issues/170
508
509 ● The cveform.mitre.org "Vendor of Product" field was set to:
510 https://github.com/cesanta/mjs
511
512 ● The cveform.mitre.org "Affected Product Code Base" field was
513 set to: mjs ES6 (JavaScript version 6)
514
515 ● The cveform.mitre.org "Suggested description" field was set
516 to: An issue was discovered in mjs(mJS: Restricted JavaScript
517 engine), ES6 (JavaScript version 6). There is stack buffer
518 overflow at 0x7ffe9049390.
519
520 🚩 The cveform.mitre.org 1001319 submission was from:
521 cfenicey@gmail.com
522 -----
523 13, For NULL pointer dereference in mjs ES6 (github issue 162) use:
524
525 CVE-2021-33449
526
527 Suggested Description:
528
529 An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_bc
530
531 Additional Information:
532
533 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set
534 to: NULL pointer dereference
535
536 ● The cveform.mitre.org "Affected Component" field was set to:
537 mjs.c, mjs_bcode_part_get_by_offset(), mjs.
538
539 ● The cveform.mitre.org "Attack Type" field was set to: Local
540
541 ● The cveform.mitre.org "Impact Denial of Service" field was
542 set to: true
543
544 ● The cveform.mitre.org "Attack Vectors" field was set to: To
545 exploit vulnerability, someone must open a crafted file, like
546 https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-7945-
547 mjs_bcode_part_get_by_offset-null-pointer-deref
548
549 ● The cveform.mitre.org "Reference" field was set to:
550 https://github.com/cesanta/mjs/issues/162
551
552 ● The cveform.mitre.org "Vendor of Product" field was set to:
553 https://github.com/cesanta/mjs
554
555 ● The cveform.mitre.org "Affected Product Code Base" field was
556 set to: mjs ES6 (JavaScript version 6)
557
558 ● The cveform.mitre.org "Suggested description" field was set
559 to: An issue was discovered in mjs(mJS: Restricted JavaScript
560 engine), ES6 (JavaScript version 6). There is NULL pointer
561 dereference in mjs_bcode_part_get_by_offset() in mjs.c.
562
563 🚩 The cveform.mitre.org 1001319 submission was from:
564 cfenicey@gmail.com
565 -----
566 14, For memory leak in NASM 2.16rc0 (id=3392758) use:
567
568 CVE-2021-33450
569
570
```

571 Suggested Description:

572

573 An issue was discovered in NASM version 2.16rc0. There are memory leaks in `nasm_malloc()` in `nasmlib/alloc.c`.

574

575 Additional Information:

576

577  ● The cveform.mitre.org "VulnerabilityType Other" field was set

578 to: memory leak

579

580 ● The cveform.mitre.org "Affected Component" field was set to:

581 `nasmlib/alloc.c, nasm_malloc(), nasm.`

582

583 ● The cveform.mitre.org "Attack Type" field was set to: Local

584

585 ● The cveform.mitre.org "Impact Denial of Service" field was

586 set to: true

587

588 ● The cveform.mitre.org "Attack Vectors" field was set to: To

589 exploit vulnerability, someone must open a crafted file, like

590 [https://github.com/Clingto/POC/blob/master/MSA/nasm/nasm-nasm](https://github.com/Clingto/POC/blob/master/MSA/nasm/nasm-nasm_malloc-1255)

591 [m\\_malloc-1255](https://github.com/Clingto/POC/blob/master/MSA/nasm/nasm-nasm_malloc-1255)

592

593 ● The cveform.mitre.org "Reference" field was set to:

594 [https://bugzilla.nasm.us/show\\_bug.cgi?id=3392758](https://bugzilla.nasm.us/show_bug.cgi?id=3392758)

595

596 ● The cveform.mitre.org "Vendor of Product" field was set to:

597 <https://github.com/netwide-assembler/nasm>

598

599 ● The cveform.mitre.org "Affected Product Code Base" field was

600 set to: NASM 2.16rc0

601

602 ● The cveform.mitre.org "Suggested description" field was set

603 to: An issue was discovered in NASM version 2.16rc0. There

604 are memory leaks in `nasm_malloc()` in `nasmlib/alloc.c`.

605

606  The cveform.mitre.org 1001319 submission was from:

607 `cfenicey@gmail.com`

608 -----

609 15. For memory leak in lrzip 0.641 use:

610

611 CVE-2021-33451

612

613 Suggested Description:

614

615 An issue was discovered in lrzip version 0.641. There are memory leaks in `fill_buffer()` in `stream.c`.

616

617 Additional Information:

618

619  ● The cveform.mitre.org "VulnerabilityType Other" field was set

620 to: memory leak

621

622 ● The cveform.mitre.org "Affected Component" field was set to:

623 `stream.c:1538, fill_buffer(), lrzip.`

624

625 ● The cveform.mitre.org "Attack Type" field was set to: Local

626

627 ● The cveform.mitre.org "Impact Denial of Service" field was

628 set to: true

629

630 ● The cveform.mitre.org "Attack Vectors" field was set to: To

631 exploit vulnerability, someone must open a crafted file, like

632 [https://github.com/Clingto/POC/blob/master/MSA/lrzip/lrzip-5](https://github.com/Clingto/POC/blob/master/MSA/lrzip/lrzip-561-fill_buffer-memory-leak)

633 [61-fill\\_buffer-memory-leak](https://github.com/Clingto/POC/blob/master/MSA/lrzip/lrzip-561-fill_buffer-memory-leak)

634

635 ● The cveform.mitre.org "Reference" field was set to:

636 <https://github.com/ckolivas/lrzip/issues/198>

637

638 ● The cveform.mitre.org "Vendor of Product" field was set to:

639 <https://github.com/ckolivas/lrzip>

640

641 ● The cveform.mitre.org "Affected Product Code Base" field was

642 set to: lrzip 0.641

643

644 ● The cveform.mitre.org "Suggested description" field was set

645 to: An issue was discovered in lrzip version 0.641. There are

646 memory leaks in `fill_buffer()` in `stream.c`.

647

648  The cveform.mitre.org 1001319 submission was from:

649 `cfenicey@gmail.com`

650 -----

651 16. For memory leak in NASM 2.16rc0 (id=3392757) use:

652

653 CVE-2021-33452

654

655 Suggested Description:

656

657 An issue was discovered in NASM version 2.16rc0. There are memory leaks in `nasm_malloc()` in `nasmlib/alloc.c`.

658

659 Additional Information:

660

661  ● The cveform.mitre.org "VulnerabilityType Other" field was set

662 to: memory leak

663

664 ● The cveform.mitre.org "Affected Component" field was set to:

665 `nasmlib/alloc.c, nasm_malloc(), nasm.`

666

667 ● The cveform.mitre.org "Attack Type" field was set to: Local

668

669 ● The cveform.mitre.org "Impact Denial of Service" field was  
670 set to: true  
671  
672 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
673 exploit vulnerability, someone must open a crafted file, like  
674 <https://github.com/Clingto/POC/blob/master/MSA/nasm/nasm-pre>  
675 [proc-4646-nasm\\_malloc-memory-leak](https://github.com/Clingto/POC/blob/master/MSA/nasm/nasm-pre)  
676  
677 ● The cveform.mitre.org "Reference" field was set to:  
678 [https://bugzilla.nasm.us/show\\_bug.cgi?id=3392757](https://bugzilla.nasm.us/show_bug.cgi?id=3392757)  
679  
680 ● The cveform.mitre.org "Vendor of Product" field was set to:  
681 <https://github.com/netwide-assembler/nasm>  
682  
683 ● The cveform.mitre.org "Affected Product Code Base" field was  
684 set to: NASM 2.16rc0  
685  
686 ● The cveform.mitre.org "Suggested description" field was set  
687 to: An issue was discovered in NASM version 2.16rc0. There  
688 are memory leaks in `nasm_malloc()` in `nasmlib/alloc.c`.  
689  
690 🚩 The cveform.mitre.org 1001319 submission was from:  
691 [cfenicey@gmail.com](mailto:cfenicey@gmail.com)  
692 -----  
693 17. For use-after-free in `lrzip 0.641` use:  
694  
695 CVE-2021-33453  
696  
697 Suggested Description:  
698  
699 An issue was discovered in `lrzip` version 0.641. There is a use-after-free in `ucompthread()` in `stream.c:1538`.  
700  
701 Additional Information:  
702  
703 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set  
704 to: NULL pointer dereference  
705  
706 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set  
707 to: use-after-free  
708  
709 ● The cveform.mitre.org "Affected Component" field was set to:  
710 `stream.c, ucompthread(), lrzip`.  
711  
712 ● The cveform.mitre.org "Attack Type" field was set to: Local  
713  
714 ● The cveform.mitre.org "Impact Denial of Service" field was  
715 set to: true  
716  
717 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
718 exploit vulnerability, someone must open a crafted file, like  
719 <https://github.com/Clingto/POC/blob/master/MSA/lrzip/lrzip-6>  
720 [02-ucompthread-UAF](https://github.com/Clingto/POC/blob/master/MSA/lrzip/lrzip-6)  
721  
722 ● The cveform.mitre.org "Reference" field was set to:  
723 <https://github.com/ckolivas/lrzip/issues/199>  
724  
725 ● The cveform.mitre.org "Vendor of Product" field was set to:  
726 <https://github.com/ckolivas/lrzip>  
727  
728 ● The cveform.mitre.org "Affected Product Code Base" field was  
729 set to: `lrzip 0.641`  
730  
731 ● The cveform.mitre.org "Suggested description" field was set  
732 to: An issue was discovered in `lrzip` version 0.641. There is  
733 a use-after-free in `ucompthread()` in `stream.c:1538`.  
734  
735 🚩 The cveform.mitre.org 1001319 submission was from:  
736 [cfenicey@gmail.com](mailto:cfenicey@gmail.com)  
737 -----  
738 18. For NULL pointer dereference in `YASM 1.3.0` (github issue 166) use:  
739  
740 CVE-2021-33454  
741  
742 Suggested Description:  
743  
744 An issue was discovered in `yasm` version 1.3.0. There is a NULL pointer dereference in `yasm_expr_get_intnum()` in `libyasm/expr.c`.  
745  
746 Additional Information:  
747  
748 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set  
749 to: NULL pointer dereference  
750  
751 ● The cveform.mitre.org "Affected Component" field was set to:  
752 `libyasm/expr.c, yasm_expr_get_intnum(), yasm`.  
753  
754 ● The cveform.mitre.org "Attack Type" field was set to: Local  
755  
756 ● The cveform.mitre.org "Impact Denial of Service" field was  
757 set to: true  
758  
759 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
760 exploit vulnerability, someone must open a crafted file, like  
761 <https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-137>  
762 [7-yasm\\_expr\\_get\\_intnum-null-pointer-deref](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-137)  
763  
764 ● The cveform.mitre.org "Reference" field was set to:  
765 <https://github.com/yasm/yasm/issues/166>  
766



767 ● The cveform.mitre.org "Vendor of Product" field was set to:  
768 <https://github.com/yasm/yasm>  
769  
770 ● The cveform.mitre.org "Affected Product Code Base" field was  
771 set to: YASM 1.3.0  
772  
773 ● The cveform.mitre.org "Suggested description" field was set  
774 to: An issue was discovered in yasm version 1.3.0. There is a  
775 NULL pointer dereference in yasm\_expr\_get\_intnum() in  
776 libyasm/expr.c.  
777  
778 🚩 The cveform.mitre.org 1001319 submission was from:  
779 cfenicey@gmail.com  
780 -----  
781 19, For NULL pointer dereference in YASM 1.3.0 (github issue 169) use:  
782  
783 CVE-2021-33455  
784  
785 Suggested Description:  
786  
787 An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in do\_directive() in modules/preprocs/nasm/nasm-pp.c.  
788  
789 Additional Information:  
790  
791 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set  
792 to: NULL pointer dereference  
793  
794 ● The cveform.mitre.org "Affected Component" field was set to:  
795 modules/preprocs/nasm/nasm-pp.c, do\_directive(), yasm.  
796  
797 ● The cveform.mitre.org "Attack Type" field was set to: Local  
798  
799 ● The cveform.mitre.org "Impact Denial of Service" field was  
800 set to: true  
801  
802 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
803 exploit vulnerability, someone must open a crafted file, like  
804 <https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-235>  
805 2-do\_directive-null-pointer-deref  
806  
807 ● The cveform.mitre.org "Reference" field was set to:  
808 <https://github.com/yasm/yasm/issues/169>  
809  
810 ● The cveform.mitre.org "Vendor of Product" field was set to:  
811 <https://github.com/yasm/yasm>  
812  
813 ● The cveform.mitre.org "Affected Product Code Base" field was  
814 set to: YASM 1.3.0  
815  
816 ● The cveform.mitre.org "Suggested description" field was set  
817 to: An issue was discovered in yasm version 1.3.0. There is a  
818 NULL pointer dereference in do\_directive() in  
819 modules/preprocs/nasm/nasm-pp.c.  
820  
821 🚩 The cveform.mitre.org 1001319 submission was from:  
822 cfenicey@gmail.com  
823 -----  
824 20, For NULL pointer dereference in YASM 1.3.0 (github issue 175) use:  
825  
826 CVE-2021-33456  
827  
828 Suggested Description:  
829  
830 An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in hash() in modules/preprocs/nasm/nasm-pp.c.  
831  
832 Additional Information:  
833  
834 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set  
835 to: NULL pointer dereference  
836  
837 ● The cveform.mitre.org "Affected Component" field was set to:  
838 modules/preprocs/nasm/nasm-pp.c, hash(), yasm.  
839  
840 ● The cveform.mitre.org "Attack Type" field was set to: Local  
841  
842 ● The cveform.mitre.org "Impact Denial of Service" field was  
843 set to: true  
844  
845 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
846 exploit vulnerability, someone must open a crafted file, like  
847 <https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-111>  
848 4-hash-null-pointer-deref  
849  
850 ● The cveform.mitre.org "Reference" field was set to:  
851 <https://github.com/yasm/yasm/issues/175>  
852  
853 ● The cveform.mitre.org "Vendor of Product" field was set to:  
854 <https://github.com/yasm/yasm>  
855  
856 ● The cveform.mitre.org "Affected Product Code Base" field was  
857 set to: YASM 1.3.0  
858  
859 ● The cveform.mitre.org "Suggested description" field was set  
860 to: An issue was discovered in yasm version 1.3.0. There is a  
861 NULL pointer dereference in hash() in  
862 modules/preprocs/nasm/nasm-pp.c.  
863  
864 🚩 The cveform.mitre.org 1001319 submission was from:

```
865 cfenicey@gmail.com
866 -----
867 21, For NULL pointer dereference in YASM 1.3.0 (github issue 171) use:
868
869 CVE-2021-33457
870
871 Suggested Description:
872
873 An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in expand_mmac_params() in modules/preprocs/nasm/nasm-pp
874
875 Additional Information:
876
877 🛡️ ● The cveform.mitre.org "VulnerabilityType Other" field was set
878 to: NULL pointer dereference
879
880 ● The cveform.mitre.org "Affected Component" field was set to:
881 modules/preprocs/nasm/nasm-pp.c, expand_mmac_params(), yasm.
882
883 ● The cveform.mitre.org "Attack Type" field was set to: Local
884
885 ● The cveform.mitre.org "Impact Denial of Service" field was
886 set to: true
887
888 ● The cveform.mitre.org "Attack Vectors" field was set to: To
889 exploit vulnerability, someone must open a crafted file, like
890 https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-385
891 7-expand_mmac_params-null-pointer-deref
892
893 ● The cveform.mitre.org "Reference" field was set to:
894 https://github.com/yasm/yasm/issues/171
895
896 ● The cveform.mitre.org "Vendor of Product" field was set to:
897 https://github.com/yasm/yasm
898
899 ● The cveform.mitre.org "Affected Product Code Base" field was
900 set to: YASM 1.3.0
901
902 ● The cveform.mitre.org "Suggested description" field was set
903 to: An issue was discovered in yasm version 1.3.0. There is a
904 NULL pointer dereference in expand_mmac_params() in
905 modules/preprocs/nasm/nasm-pp.c.
906
907 🏆 The cveform.mitre.org 1001319 submission was from:
908 cfenicey@gmail.com
909 -----
910 22, For NULL pointer dereference in YASM 1.3.0 (github issue 170) use:
911
912 CVE-2021-33458
913
914 Suggested Description:
915
916 An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in find_cc() in modules/preprocs/nasm/nasm-pp.c.
917
918 Additional Information:
919
920 🛡️ ● The cveform.mitre.org "VulnerabilityType Other" field was set
921 to: NULL pointer dereference
922
923 ● The cveform.mitre.org "Affected Component" field was set to:
924 modules/preprocs/nasm/nasm-pp.c, find_cc(), yasm.
925
926 ● The cveform.mitre.org "Attack Type" field was set to: Local
927
928 ● The cveform.mitre.org "Impact Denial of Service" field was
929 set to: true
930
931 ● The cveform.mitre.org "Attack Vectors" field was set to: To
932 exploit vulnerability, someone must open a crafted file, like
933 https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-381
934 1-find_cc-null-pointer-deref
935
936 ● The cveform.mitre.org "Reference" field was set to:
937 https://github.com/yasm/yasm/issues/170
938
939 ● The cveform.mitre.org "Vendor of Product" field was set to:
940 https://github.com/yasm/yasm
941
942 ● The cveform.mitre.org "Affected Product Code Base" field was
943 set to: YASM 1.3.0
944
945 ● The cveform.mitre.org "Suggested description" field was set
946 to: An issue was discovered in yasm version 1.3.0. There is a
947 NULL pointer dereference in find_cc() in
948 modules/preprocs/nasm/nasm-pp.c.
949
950 🏆 The cveform.mitre.org 1001319 submission was from:
951 cfenicey@gmail.com
952 -----
953 23, For NULL pointer dereference in YASM 1.3.0 (github issue 167) use:
954
955 CVE-2021-33459
956
957 Suggested Description:
958
959 An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in nasm_parser_directive() in modules/parsers/nasm/nasm-
960
961 Additional Information:
962
```

963  ● The cveform.mitre.org "VulnerabilityType Other" field was set  
964 to: NULL pointer dereference  
965  
966 ● The cveform.mitre.org "Affected Component" field was set to:  
967 modules/parsers/nasm/nasm-parse.c, nasm\_parser\_directive(),  
968 yasm.  
969  
970 ● The cveform.mitre.org "Attack Type" field was set to: Local  
971  
972 ● The cveform.mitre.org "Impact Denial of Service" field was  
973 set to: true  
974  
975 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
976 exploit vulnerability, someone must open a crafted file, like  
977 [https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-159](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-1595-nasm_parser_directive-null-pointer-deref)  
978 [5-nasm\\_parser\\_directive-null-pointer-deref](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-1595-nasm_parser_directive-null-pointer-deref)  
979  
980 ● The cveform.mitre.org "Reference" field was set to:  
981 <https://github.com/yasm/yasm/issues/167>  
982  
983 ● The cveform.mitre.org "Vendor of Product" field was set to:  
984 <https://github.com/yasm/yasm>  
985  
986 ● The cveform.mitre.org "Affected Product Code Base" field was  
987 set to: YASM 1.3.0  
988  
989 ● The cveform.mitre.org "Suggested description" field was set  
990 to: An issue was discovered in yasm version 1.3.0. There is a  
991 NULL pointer dereference in nasm\_parser\_directive() in  
992 modules/parsers/nasm/nasm-parse.c.  
993  
994  The cveform.mitre.org 1001319 submission was from:  
995 cfenicey@gmail.com  
996 -----  
997 24, For NULL pointer dereference in YASM 1.3.0 (github issue 168) use:  
998  
999 CVE-2021-33460  
1000  
1001 Suggested Description:  
1002  
1003 An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in if\_condition() in modules/preprocs/nasm/nasm-pp.c.  
1004  
1005 Additional Information:  
1006  
1007  ● The cveform.mitre.org "VulnerabilityType Other" field was set  
1008 to: NULL pointer dereference  
1009  
1010 ● The cveform.mitre.org "Affected Component" field was set to:  
1011 modules/preprocs/nasm/nasm-pp.c, if\_condition(), yasm.  
1012  
1013 ● The cveform.mitre.org "Attack Type" field was set to: Local  
1014  
1015 ● The cveform.mitre.org "Impact Denial of Service" field was  
1016 set to: true  
1017  
1018 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
1019 exploit vulnerability, someone must open a crafted file, like  
1020 [https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-213](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-2134-if_condition-null-pointer-deref)  
1021 [4-if\\_condition-null-pointer-deref](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-2134-if_condition-null-pointer-deref)  
1022  
1023 ● The cveform.mitre.org "Reference" field was set to:  
1024 <https://github.com/yasm/yasm/issues/168>  
1025  
1026 ● The cveform.mitre.org "Vendor of Product" field was set to:  
1027 <https://github.com/yasm/yasm>  
1028  
1029 ● The cveform.mitre.org "Affected Product Code Base" field was  
1030 set to: YASM 1.3.0  
1031  
1032 ● The cveform.mitre.org "Suggested description" field was set  
1033 to: An issue was discovered in yasm version 1.3.0. There is a  
1034 NULL pointer dereference in if\_condition() in  
1035 modules/preprocs/nasm/nasm-pp.c.  
1036  
1037  The cveform.mitre.org 1001319 submission was from:  
1038 cfenicey@gmail.com  
1039 -----  
1040 25, For use-after-free in YASM 1.3.0 (github issue 161) use:  
1041  
1042 CVE-2021-33461  
1043  
1044 Suggested Description:  
1045  
1046 An issue was discovered in yasm version 1.3.0. There is a use-after-free in yasm\_intnum\_destroy() in libyasm/intnum.c.  
1047  
1048 Additional Information:  
1049  
1050  ● The cveform.mitre.org "VulnerabilityType Other" field was set  
1051 to: use-after-free  
1052  
1053 ● The cveform.mitre.org "Affected Component" field was set to:  
1054 libyasm/intnum.c, yasm\_intnum\_destroy(), yasm.  
1055  
1056 ● The cveform.mitre.org "Attack Type" field was set to: Local  
1057  
1058 ● The cveform.mitre.org "Impact Denial of Service" field was  
1059 set to: true  
1060

1061 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
1062 exploit vulnerability, someone must open a crafted file, like  
1063 [https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-415](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-415-yasm_intnum_destroy-UAF)  
1064 -yasm\_intnum\_destroy-UAF  
1065  
1066 ● The cveform.mitre.org "Reference" field was set to:  
1067 <https://github.com/yasm/yasm/issues/161>  
1068  
1069 ● The cveform.mitre.org "Vendor of Product" field was set to:  
1070 <https://github.com/yasm/yasm>  
1071  
1072 ● The cveform.mitre.org "Affected Product Code Base" field was  
1073 set to: YASM 1.3.0  
1074  
1075 ● The cveform.mitre.org "Suggested description" field was set  
1076 to: An issue was discovered in yasm version 1.3.0. There is a  
1077 use-after-free in yasm\_intnum\_destroy() in libyasm/intnum.c.  
1078  
1079 🚩 The cveform.mitre.org 1001319 submission was from:  
1080 cfenicey@gmail.com  
1081 -----  
1082 26, For use-after-free in YASM 1.3.0 (github issue 165) use:  
1083  
1084 CVE-2021-33462  
1085  
1086 Suggested Description:  
1087  
1088 An issue was discovered in yasm version 1.3.0. There is a use-after-free in expr\_traverse\_nodes\_post() in libyasm/expr.c.  
1089  
1090 Additional Information:  
1091  
1092 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set  
1093 to: use-after-free  
1094  
1095 ● The cveform.mitre.org "Affected Component" field was set to:  
1096 libyasm/expr.c, expr\_traverse\_nodes\_post(), yasm.  
1097  
1098 ● The cveform.mitre.org "Attack Type" field was set to: Local  
1099  
1100 ● The cveform.mitre.org "Impact Denial of Service" field was  
1101 set to: true  
1102  
1103 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
1104 exploit vulnerability, someone must open a crafted file, like  
1105 [https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-122](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-122-6-expr_traverse_nodes_post-UAF)  
1106 6-expr\_traverse\_nodes\_post-UAF  
1107  
1108 ● The cveform.mitre.org "Reference" field was set to:  
1109 <https://github.com/yasm/yasm/issues/165>  
1110  
1111 ● The cveform.mitre.org "Vendor of Product" field was set to:  
1112 <https://github.com/yasm/yasm>  
1113  
1114 ● The cveform.mitre.org "Affected Product Code Base" field was  
1115 set to: YASM 1.3.0  
1116  
1117 ● The cveform.mitre.org "Suggested description" field was set  
1118 to: An issue was discovered in yasm version 1.3.0. There is a  
1119 use-after-free in expr\_traverse\_nodes\_post() in  
1120 libyasm/expr.c.  
1121  
1122 🚩 The cveform.mitre.org 1001319 submission was from:  
1123 cfenicey@gmail.com  
1124 -----  
1125 27, For NULL pointer dereference in YASM 1.3.0 (github issue 174) use:  
1126  
1127 CVE-2021-33463  
1128  
1129 Suggested Description:  
1130  
1131 An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in yasm\_expr\_\_copy\_except() in libyasm/expr.c.  
1132  
1133 Additional Information:  
1134  
1135 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set  
1136 to: NULL pointer dereference  
1137  
1138 ● The cveform.mitre.org "Affected Component" field was set to:  
1139 libyasm/expr.c, yasm\_expr\_\_copy\_except(), yasm.  
1140  
1141 ● The cveform.mitre.org "Attack Type" field was set to: Local  
1142  
1143 ● The cveform.mitre.org "Impact Denial of Service" field was  
1144 set to: true  
1145  
1146 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
1147 exploit vulnerability, someone must open a crafted file, like  
1148 [https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-111](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-1113-yasm_expr__copy_except-null-pointer-deref)  
1149 3-yasm\_expr\_\_copy\_except-null-pointer-deref  
1150  
1151 ● The cveform.mitre.org "Reference" field was set to:  
1152 <https://github.com/yasm/yasm/issues/174>  
1153  
1154 ● The cveform.mitre.org "Vendor of Product" field was set to:  
1155 <https://github.com/yasm/yasm>  
1156  
1157 ● The cveform.mitre.org "Affected Product Code Base" field was  
1158 set to: YASM 1.3.0

```
1159
1160 ● The cveform.mitre.org "Suggested description" field was set
1161 to: An issue was discovered in yasm version 1.3.0. There is a
1162 NULL pointer dereference in yasm_expr__copy_except() in
1163 libyasm/expr.c.
1164
1165 🚩 The cveform.mitre.org 1001319 submission was from:
1166 cfenicey@gmail.com
1167 -----
1168 28, For heap buffer overflow in YASM 1.3.0 (github issue 164) use:
1169
1170 CVE-2021-33464
1171
1172 Suggested Description:
1173
1174 An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in inc_fopen() in modules/preprocs/nasm/nasm-pp.c.
1175
1176 Additional Information:
1177
1178 🚩 ● The cveform.mitre.org "Vulnerability Type" field was set to:
1179 Buffer Overflow
1180
1181 ● The cveform.mitre.org "Affected Component" field was set to:
1182 modules/preprocs/nasm/nasm-pp.c, inc_fopen(), yasm.
1183
1184 ● The cveform.mitre.org "Attack Type" field was set to: Local
1185
1186 ● The cveform.mitre.org "Impact Denial of Service" field was
1187 set to: true
1188
1189 ● The cveform.mitre.org "Attack Vectors" field was set to: To
1190 exploit vulnerability, someone must open a crafted file, like
1191 https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-730
1192 6d-inc_fopen-heap-buffer-overflow
1193
1194 ● The cveform.mitre.org "Reference" field was set to:
1195 https://github.com/yasm/yasm/issues/164
1196
1197 ● The cveform.mitre.org "Vendor of Product" field was set to:
1198 https://github.com/yasm/yasm
1199
1200 ● The cveform.mitre.org "Affected Product Code Base" field was
1201 set to: YASM 1.3.0
1202
1203 ● The cveform.mitre.org "Suggested description" field was set
1204 to: An issue was discovered in yasm version 1.3.0. There is a
1205 heap-buffer-overflow in inc_fopen() in
1206 modules/preprocs/nasm/nasm-pp.c.
1207
1208 🚩 The cveform.mitre.org 1001319 submission was from:
1209 cfenicey@gmail.com
1210 -----
1211 29, For NULL pointer dereference in YASM 1.3.0 (github issue 173) use:
1212
1213 CVE-2021-33465
1214
1215 Suggested Description:
1216
1217 An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in expand_mmacro() in modules/preprocs/nasm/nasm-pp.c.
1218
1219 Additional Information:
1220
1221 🚩 ● The cveform.mitre.org "VulnerabilityType Other" field was set
1222 to: NULL pointer dereference
1223
1224 ● The cveform.mitre.org "Affected Component" field was set to:
1225 modules/preprocs/nasm/nasm-pp.c, expand_mmacro(), yasm.
1226
1227 ● The cveform.mitre.org "Attack Type" field was set to: Local
1228
1229 ● The cveform.mitre.org "Impact Denial of Service" field was
1230 set to: true
1231
1232 ● The cveform.mitre.org "Attack Vectors" field was set to: To
1233 exploit vulnerability, someone must open a crafted file, like
1234 https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-476
1235 0-expand_mmacro-null-pointer-deref
1236
1237 ● The cveform.mitre.org "Reference" field was set to:
1238 https://github.com/yasm/yasm/issues/173
1239
1240 ● The cveform.mitre.org "Vendor of Product" field was set to:
1241 https://github.com/yasm/yasm
1242
1243 ● The cveform.mitre.org "Affected Product Code Base" field was
1244 set to: YASM 1.3.0
1245
1246 ● The cveform.mitre.org "Suggested description" field was set
1247 to: An issue was discovered in yasm version 1.3.0. There is a
1248 NULL pointer dereference in expand_mmacro() in
1249 modules/preprocs/nasm/nasm-pp.c.
1250
1251 🚩 The cveform.mitre.org 1001319 submission was from:
1252 cfenicey@gmail.com
1253 -----
1254 30, For NULL pointer dereference in YASM 1.3.0 (github issue 172) use:
1255
1256 CVE-2021-33466
```

1257  
1258 Suggested Description:  
1259  
1260 An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in `expand_macro()` in `modules/preprocs/nasm/nasm-pp.c`.  
1261  
1262 Additional Information:  
1263  
1264 📌 ● The cveform.mitre.org "VulnerabilityType Other" field was set  
1265 to: NULL pointer dereference  
1266  
1267 ● The cveform.mitre.org "Affected Component" field was set to:  
1268 `modules/preprocs/nasm/nasm-pp.c`, `expand_macro()`, `yasm`.  
1269  
1270 ● The cveform.mitre.org "Attack Type" field was set to: Local  
1271  
1272 ● The cveform.mitre.org "Impact Denial of Service" field was  
1273 set to: true  
1274  
1275 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
1276 exploit vulnerability, someone must open a crafted file, like  
1277 <https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-435>  
1278 `2-expand_macro-null-pointer-deref`  
1279  
1280 ● The cveform.mitre.org "Reference" field was set to:  
1281 <https://github.com/yasm/yasm/issues/172>  
1282  
1283 ● The cveform.mitre.org "Vendor of Product" field was set to:  
1284 <https://github.com/yasm/yasm>  
1285  
1286 ● The cveform.mitre.org "Affected Product Code Base" field was  
1287 set to: YASM 1.3.0  
1288  
1289 ● The cveform.mitre.org "Suggested description" field was set  
1290 to: An issue was discovered in yasm version 1.3.0. There is a  
1291 NULL pointer dereference in `expand_macro()` in  
1292 `modules/preprocs/nasm/nasm-pp.c`.  
1293  
1294 📌 The cveform.mitre.org 1001319 submission was from:  
1295 `cfenicey@gmail.com`  
1296 -----  
1297 31, For use-after-free in YASM 1.3.0 (github issue 163) use:  
1298  
1299 CVE-2021-33467  
1300  
1301 Suggested Description:  
1302  
1303 An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in `hash()` in `modules/preprocs/nasm/nasm-pp.c`.  
1304  
1305 Additional Information:  
1306  
1307 📌 ● The cveform.mitre.org "VulnerabilityType Other" field was set  
1308 to: use-after-free  
1309  
1310 ● The cveform.mitre.org "Affected Component" field was set to:  
1311 `modules/preprocs/nasm/nasm-pp.c`, `pp_getline()`, `yasm`.  
1312  
1313 ● The cveform.mitre.org "Attack Type" field was set to: Local  
1314  
1315 ● The cveform.mitre.org "Impact Denial of Service" field was  
1316 set to: true  
1317  
1318 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
1319 exploit vulnerability, someone must open a crafted file, like  
1320 <https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-502>  
1321 `0-pp_getline-UAF`  
1322  
1323 ● The cveform.mitre.org "Reference" field was set to:  
1324 <https://github.com/yasm/yasm/issues/163>  
1325  
1326 ● The cveform.mitre.org "Vendor of Product" field was set to:  
1327 <https://github.com/yasm/yasm>  
1328  
1329 ● The cveform.mitre.org "Affected Product Code Base" field was  
1330 set to: YASM 1.3.0  
1331  
1332 ● The cveform.mitre.org "Suggested description" field was set  
1333 to: An issue was discovered in yasm version 1.3.0. There is a  
1334 use-after-free in `pp_getline()` in  
1335 `modules/preprocs/nasm/nasm-pp.c`.  
1336  
1337 📌 The cveform.mitre.org 1001319 submission was from:  
1338 `cfenicey@gmail.com`  
1339 -----  
1340 32, For use-after-free in YASM 1.3.0 (github issue 162) use:  
1341  
1342 CVE-2021-33468  
1343  
1344 Suggested Description:  
1345  
1346 An issue was discovered in yasm version 1.3.0. There is a use-after-free in `error()` in `modules/preprocs/nasm/nasm-pp.c`.  
1347  
1348 Additional Information:  
1349  
1350 📌 ● The cveform.mitre.org "VulnerabilityType Other" field was set  
1351 to: use-after-free  
1352  
1353 ● The cveform.mitre.org "Affected Component" field was set to:  
1354 `modules/preprocs/nasm/nasm-pp.c`, `error()`, `yasm`.

1355  
1356 ● The cveform.mitre.org "Attack Type" field was set to: Local  
1357  
1358 ● The cveform.mitre.org "Impact Denial of Service" field was  
1359 set to: true  
1360  
1361 ● The cveform.mitre.org "Attack Vectors" field was set to: To  
1362 exploit vulnerability, someone must open a crafted file, like  
1363 [https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-482](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-4826-error-UAF)  
1364 [6-error-UAF](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-4826-error-UAF)  
1365  
1366 ● The cveform.mitre.org "Reference" field was set to:  
1367 <https://github.com/yasm/yasm/issues/162>  
1368  
1369 ● The cveform.mitre.org "Vendor of Product" field was set to:  
1370 <https://github.com/yasm/yasm>  
1371  
1372 ● The cveform.mitre.org "Affected Product Code Base" field was  
1373 set to: YASM 1.3.0  
1374  
1375 ● The cveform.mitre.org "Suggested description" field was set  
1376 to: An issue was discovered in yasm version 1.3.0. There is a  
1377 use-after-free in error() in modules/preprocs/nasm/nasm-pp.c.  
1378  
1379 🚩 The cveform.mitre.org 1001319 submission was from:  
1380 cfenicey@gmail.com  
1381 -----  
1382  
1383  
1384 Please do not hesitate to contact the CVE Team by replying to this email if you have any questions, or to provide more details.  
1385  
1386 Please do not change the subject line, which allows us to effectively track your request.  
1387  
1388 CVE Assignment Team  
1389  
1390 M/S M300, 202 Burlington Road, Bedford, MA 01730 USA  
1391  
1392 [A PGP key is available for encrypted communications at  
1393 [http://cve.mitre.org/cve/request\\_id.html](http://cve.mitre.org/cve/request_id.html)]  
1394  
1395 {CMI: MCID12019014}  
1396

