Instantly share code, notes, and snippets.

Clingto / gist:bb632c0c463f4b2c97e4f65f751c5e6d

Created 5 months ago

☆ Star

<> Code -o- Revisions 1

Minimum information for the vulnerability covered by 32 CVEs.

gistfile1.txt

```
1、For Memory Leak in mjs ES6 use:
CVE-2021-33437

Suggested Description:

An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There are memory leaks in frozen_cb() in mj

Additional Information:
⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: memory leak

● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, frozen_cb(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-5794-
frozen_cb-memory-leak

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/160

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There are memory leaks
in frozen_cb() in mjs.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com

-----------------------------------------------------------------------------------
2、For Buffer Overflow in mjs ES6 use:

CVE-2021-33438

Suggested Description:

An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is stack buffer overflow in json_pars

Additional Information:

⌛ ● The cveform.mitre.org "Vulnerability Type" field was set to:
Buffer Overflow

● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, json_parse_array(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-5fb78
-json_parse_array-stack-overflow

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/158

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is stack buffer
```

```
overflow in json_parse_array() in mjs.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com

-----------------------------------------------------------------------------------

3、For NULL pointer dereference in mjs ES6 use:

CVE-2021-33439

Suggested Description:

An issue was discovered in mjs(mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in gc_comp

Additional Information:

⏳ ● The cveform.mitre.org "Vulnerability Type" field was set to:
NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, gc_compact_strings(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-8d05d
-gc_compact_strings-negative-size-param

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/159

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is Integer
overflow in gc_compact_strings() in mjs.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------

4、For NULL pointer dereference in mjs ES6 (github issue 163) use:

CVE-2021-33440

Suggested Description:

An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_bc

Additional Information:

⏳ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, mjs_bcode_commit(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-7954-
mjs_bcode_commit-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/163

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is NULL pointer
dereference in mjs_bcode_commit() in mjs.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------

5、For NULL pointer dereference in mjs ES6 (github issue 165) use:

CVE-2021-33441
```

```

Suggested Description:

An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in exec_e

Additional Information:

⏳ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, exec_expr(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-9035-
exec_expr-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/165

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is NULL pointer
dereference in exec_expr() in mjs.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
----------------------------------------------------------------------------------

6、For NULL pointer dereference in mjs ES6 (github issue 161) use:

CVE-2021-33442

Suggested Description:

An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in json_p

Additional Information:

⏳ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, json_printf(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-6368-
json_printf-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/161

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is NULL pointer
dereference in json_printf() in mjs.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
----------------------------------------------------------------------------------

7、For NULL pointer dereference in mjs ES6 (github issue 167) use:

CVE-2021-33443

Suggested Description:

An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is stack buffer overflow in mjs_execu

Additional Information:

⏳ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

```

```
● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, mjs_execute(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-9522-
mjs_execute-stack-overflow

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/167

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is stack buffer
overflow in mjs_execute() in mjs.c.

⛹️ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------

8、For NULL pointer dereference in mjs ES6 (github issue 166) use:

CVE-2021-33444

Suggested Description:

An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in getpro

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, getprop_builtin_foreign(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-9187-
getprop_builtin_foreign-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/166

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is NULL pointer
dereference in getprop_builtin_foreign() in mjs.c.

⛹️ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------

9、For NULL pointer dereference in mjs ES6 (github issue 169) use:

CVE-2021-33445

Suggested Description:

An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_st

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, mjs_string_char_code_at(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
```

```
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-13891
-mjs_string_char_code_at-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/169

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is NULL pointer
dereference in mjs_string_char_code_at() in mjs.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------
10、For NULL pointer dereference in mjs ES6 (github issue 168) use:

CVE-2021-33446

Suggested Description:

An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_ne

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, mjs_next(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-12318
-mjs_next-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/168

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is NULL pointer
dereference in mjs_next() in mjs.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------
11、For NULL pointer dereference in mjs ES6 (github issue 164) use:

CVE-2021-33447

Suggested Description:

An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_pr

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, mjs_print(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-7992-
mjs_print-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/164

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

```

```
● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is NULL pointer
dereference in mjs_print() in mjs.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------
12、For Buffer Overflow in mjs ES6 (github issue 170) use:

CVE-2021-33448

Suggested Description:

An issue was discovered in mjs(mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is stack buffer overflow at 0x7fffe904

Additional Information:

⏳ ● The cveform.mitre.org "Vulnerability Type" field was set to:
Buffer Overflow

● The cveform.mitre.org "Affected Component" field was set to:
<unknown module>, at 0x7fffe9049390, mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-modul
e-stack-overflow

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/170

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is stack buffer
overflow at 0x7fffe9049390.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------
13、For NULL pointer dereference in mjs ES6 (github issue 162) use:

CVE-2021-33449

Suggested Description:

An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_bc

Additional Information:

⏳ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
mjs.c, mjs_bcode_part_get_by_offset(), mjs.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-7945-
mjs_bcode_part_get_by_offset-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/cesanta/mjs/issues/162

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/cesanta/mjs

● The cveform.mitre.org "Affected Product Code Base" field was
set to: mjs ES6 (JavaScript version 6)

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in mjs(mJS: Restricted JavaScript
engine), ES6 (JavaScript version 6). There is NULL pointer
dereference in mjs_bcode_part_get_by_offset() in mjs.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------
14、For memory leak in NASM 2.16rc0 (id=3392758) use:

CVE-2021-33450

```

```
Suggested Description:

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

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: memory leak

● The cveform.mitre.org "Affected Component" field was set to:
nasmlib/alloc.c, nasm_calloc(), nasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/nasm/nasm-nas
m_calloc-1255

● The cveform.mitre.org "Reference" field was set to:
https://bugzilla.nasm.us/show_bug.cgi?id=3392758

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/netwide-assembler/nasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: NASM 2.16rc0

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in NASM version 2.16rc0. There
are memory leaks in nasm_calloc() in nasmlib/alloc.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
----------------------------------------------------------------------------------
15、For memory leak in lrzip 0.641 use:

CVE-2021-33451

Suggested Description:

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

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: memory leak

● The cveform.mitre.org "Affected Component" field was set to:
stream.c:1538, fill_buffer(), lrzip.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/lrzip/lrzip-5
61-fill_buffer-memory-leak

● The cveform.mitre.org "Reference" field was set to:
https://github.com/ckolivas/lrzip/issues/198

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/ckolivas/lrzip

● The cveform.mitre.org "Affected Product Code Base" field was
set to: lrzip 0.641

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in lrzip version 0.641. There are
memory leaks in fill_buffer() in stream.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
----------------------------------------------------------------------------------
16、For memory leak in NASM 2.16rc0 (id=3392757) use:

CVE-2021-33452

Suggested Description:

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

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: memory leak

● The cveform.mitre.org "Affected Component" field was set to:
nasmlib/alloc.c, nasm_malloc(), nasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/nasm/nasm-pre
proc-4646-nasm_malloc-memory-leak

● The cveform.mitre.org "Reference" field was set to:
https://bugzilla.nasm.us/show_bug.cgi?id=3392757

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/netwide-assembler/nasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: NASM 2.16rc0

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in NASM version 2.16rc0. There
are memory leaks in nasm_malloc() in nasmlib/alloc.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
--------------------------------------------------------------------------------
17、For use-after-free in lrzip 0.641 use:

CVE-2021-33453

Suggested Description:

An issue was discovered in lrzip version 0.641. There is a use-after-free in ucompthread() in stream.c:1538.

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: use-after-free

● The cveform.mitre.org "Affected Component" field was set to:
stream.c, ucompthread(), lrzip.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/lrzip/lrzip-6
02-ucompthread-UAF

● The cveform.mitre.org "Reference" field was set to:
https://github.com/ckolivas/lrzip/issues/199

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/ckolivas/lrzip

● The cveform.mitre.org "Affected Product Code Base" field was
set to: lrzip 0.641

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in lrzip version 0.641. There is
a use-after-free in ucompthread() in stream.c:1538.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
--------------------------------------------------------------------------------
18、For NULL pointer dereference in YASM 1.3.0 (github issue 166) use:

CVE-2021-33454

Suggested Description:

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.

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
libyasm/expr.c, yasm_expr_get_intnum(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-137
7-yasm_expr_get_intnum-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/166

```

```
● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

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

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
----------------------------------------------------------------------------------
19、For NULL pointer dereference in YASM 1.3.0 (github issue 169) use:

CVE-2021-33455

Suggested Description:

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.

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
modules/preprocs/nasm/nasm-pp.c, do_directive(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-235
2-do_directive-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/169

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

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

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
----------------------------------------------------------------------------------
20、For NULL pointer dereference in YASM 1.3.0 (github issue 175) use:

CVE-2021-33456

Suggested Description:

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.

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
modules/preprocs/nasm/nasm-pp.c, hash(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability,someone must open a crafted file,like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-111
4-hash-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/175

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

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

⛹ The cveform.mitre.org 1001319 submission was from:
```

```
cfenicey@gmail.com
----------------------------------------------------------------------------------
21、For NULL pointer dereference in YASM 1.3.0 (github issue 171) use:

CVE-2021-33457

Suggested Description:

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

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
modules/preprocs/nasm/nasm-pp.c, expand_mmac_params(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-385
7-expand_mmac_params-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/171

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

● The cveform.mitre.org "Suggested description" field was set
to: 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.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
----------------------------------------------------------------------------------
22、For NULL pointer dereference in YASM 1.3.0 (github issue 170) use:

CVE-2021-33458

Suggested Description:

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.

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
modules/preprocs/nasm/nasm-pp.c, find_cc(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-381
1-find_cc-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/170

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

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

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
----------------------------------------------------------------------------------
23、For NULL pointer dereference in YASM 1.3.0 (github issue 167) use:

CVE-2021-33459

Suggested Description:

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-

Additional Information:

```

```
⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
modules/parsers/nasm/nasm-parse.c, nasm_parser_directive(),
yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-159
5-nasm_parser_directive-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/167

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

● The cveform.mitre.org "Suggested description" field was set
to: 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-parse.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
----------------------------------------------------------------------------------
24、For NULL pointer dereference in YASM 1.3.0 (github issue 168) use:

CVE-2021-33460

Suggested Description:

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.

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
modules/preprocs/nasm/nasm-pp.c, if_condition(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-213
4-if_condition-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/168

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

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

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
----------------------------------------------------------------------------------
25、For use-after-free in YASM 1.3.0 (github issue 161) use:

CVE-2021-33461

Suggested Description:

An issue was discovered in yasm version 1.3.0. There is a use-after-free in yasm_intnum_destroy() in libyasm/intnum.c.

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: use-after-free

● The cveform.mitre.org "Affected Component" field was set to:
libyasm/intnum.c, yasm_intnum_destroy(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

```

```
● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-415
-yasm_intnum_destroy-UAF

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/161

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in yasm version 1.3.0. There is a
use-after-free in yasm_intnum_destroy() in libyasm/intnum.c.

⛹️ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------
26、For use-after-free in YASM 1.3.0 (github issue 165) use:

CVE-2021-33462

Suggested Description:

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.

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: use-after-free

● The cveform.mitre.org "Affected Component" field was set to:
libyasm/expr.c, expr_traverse_nodes_post(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-122
6-expr_traverse_nodes_post-UAF

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/165

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

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

⛹️ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------
27、For NULL pointer dereference in YASM 1.3.0 (github issue 174) use:

CVE-2021-33463

Suggested Description:

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.

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
libyasm/expr.c, yasm_expr__copy_except(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-111
3-yasm_expr__copy_except-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/174

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0
```

```

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

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
--------------------------------------------------------------------------------
28、For heap buffer overflow in YASM 1.3.0 (github issue 164) use:

CVE-2021-33464

Suggested Description:

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.

Additional Information:

⌛ ● The cveform.mitre.org "Vulnerability Type" field was set to:
Buffer Overflow

● The cveform.mitre.org "Affected Component" field was set to:
modules/preprocs/nasm/nasm-pp.c, inc_fopen(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-730
6d-inc_fopen-heap-buffer-overflow

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/164

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in yasm version 1.3.0. There is a
heap-buffer-overflow in inc_fopen() in
modules/preprocs/nasm/nasm-pp.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
--------------------------------------------------------------------------------
29、For NULL pointer dereference in YASM 1.3.0 (github issue 173) use:

CVE-2021-33465

Suggested Description:

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.

Additional Information:

⌛ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
modules/preprocs/nasm/nasm-pp.c, expand_mmacro(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-476
0-expand_mmacro-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/173

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

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

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
--------------------------------------------------------------------------------
30、For NULL pointer dereference in YASM 1.3.0 (github issue 172) use:

CVE-2021-33466
```

```

Suggested Description:

An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in expand_smacro() in modules/preprocs/nasm/nasm-pp.c.

Additional Information:

⏳ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: NULL pointer dereference

● The cveform.mitre.org "Affected Component" field was set to:
modules/preprocs/nasm/nasm-pp.c, expand_smacro(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-435
2-expand_smacro-null-pointer-deref

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/172

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in yasm version 1.3.0. There is a
NULL pointer dereference in expand_smacro() in
modules/preprocs/nasm/nasm-pp.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------
31、For use-after-free in YASM 1.3.0 (github issue 163) use:

CVE-2021-33467

Suggested Description:

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.

Additional Information:

⏳ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: use-after-free

● The cveform.mitre.org "Affected Component" field was set to:
modules/preprocs/nasm/nasm-pp.c, pp_getline(), yasm.

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

● The cveform.mitre.org "Impact Denial of Service" field was
set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To
exploit vulnerability, someone must open a crafted file, like
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-502
0-pp_getline-UAF

● The cveform.mitre.org "Reference" field was set to:
https://github.com/yasm/yasm/issues/163

● The cveform.mitre.org "Vendor of Product" field was set to:
https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was
set to: YASM 1.3.0

● The cveform.mitre.org "Suggested description" field was set
to: An issue was discovered in yasm version 1.3.0. There is a
use-after-free in pp_getline() in
modules/preprocs/nasm/nasm-pp.c.

⛹ The cveform.mitre.org 1001319 submission was from:
cfenicey@gmail.com
-----------------------------------------------------------------------------------
32、For use-after-free in YASM 1.3.0 (github issue 162) use:

CVE-2021-33468

Suggested Description:

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.

Additional Information:

⏳ ● The cveform.mitre.org "VulnerabilityType Other" field was set
to: use-after-free

● The cveform.mitre.org "Affected Component" field was set to:
modules/preprocs/nasm/nasm-pp.c, error(), yasm.
```

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

● The cveform.mitre.org "Impact Denial of Service" field was set to: true

● The cveform.mitre.org "Attack Vectors" field was set to: To exploit vulnerability, someone must open a crafted file, like https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-4826-error-UAF

● The cveform.mitre.org "Reference" field was set to: https://github.com/yasm/yasm/issues/162

● The cveform.mitre.org "Vendor of Product" field was set to: https://github.com/yasm/yasm

● The cveform.mitre.org "Affected Product Code Base" field was set to: YASM 1.3.0

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

The cveform.mitre.org 1001319 submission was from: cfenicey@gmail.com

----

Please do not hesitate to contact the CVE Team by replying to this email if you have any questions, or to provide more details.

Please do not change the subject line, which allows us to effectively track your request.

CVE Assignment Team

M/S M300, 202 Burlington Road, Bedford, MA 01730 USA

[A PGP key is available for encrypted communications at

http://cve.mitre.org/cve/request_id.html]

{CMI: MCID12019014}