Benchmark	CVES	#CVE
Bottleneck	**CVE-2022-34070**	**1**
Jansi	**CVE-2022-34072**	**1**
JavaParser	**CVE-2022-34073**	**1**
Ultrajson	**CVE-2022-34074**	**1**
Pillow	**CVE-2022-34075**	**1**
	Total	**5**

Subject	Ultrajson
Vulnerability Type	Segment fault
Input	mutated seed by PolyFuzz
Description	Segment fault happened with specific inputs: Program received signal SIGSEGV, Segmentation fault. PyBytes_Size () at /tmp/build/80754af9/python-split_1631797238431/work/Objects/bytesobject.c:1199 1199 /tmp/build/80754af9/python-split_1631797238431/work/Objects/bytesobject.c: No such file or directory. (gdb) bt #0 PyBytes_Size () at /tmp/build/80754af9/python-split_1631797238431/work/Objects/bytesobject.c:1199 #1 0x00007ffff7e25e99 in ?? () from /root/anaconda3/lib/python3.9/site-packages/ujson.cpython-39-x86_64-linux-gnu.so #2 0x00007ffff7e24b94 in ?? () from /root/anaconda3/lib/python3.9/site-packages/ujson.cpython-39-x86_64-linux-gnu.so #3 0x00007ffff7e253cf in JSON_EncodeObject () from /root/anaconda3/lib/python3.9/site-packages/ujson.cpython-39-x86_64-linux-gnu.so #4 0x00007ffff7e26e93 in objToJSON () from /root/anaconda3/lib/python3.9/site-packages/ujson.cpython-39-x86_64-linux-gnu.so #5 0x00005555556c8714 in cfunction_call () at /tmp/build/80754af9/python-split_1631797238431/work/Objects/methodobject.c:543 #6 0x0000555555689ef in _PyObject_MakeTpCall () at /tmp/build/80754af9/python-split_1631797238431/work/Objects/call.c:191 #7 0x0000555555722d89 in _PyObject_VectorcallTstate (kwnames=0x0,

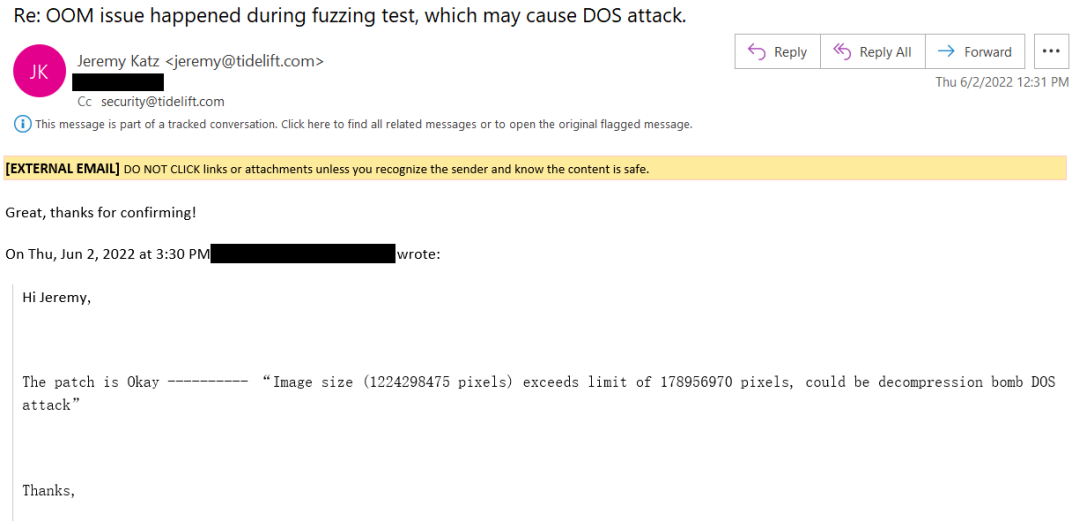
	nargsf=<optimized out>, args=0x7ffff7ed5758, callable=<optimized out>, tstate=<optimized out>) at /tmp/build/80754af9/python-split_1631797238431/work/Include/cpython/abstract.h:11
PoC	https://github.com/baltsers/polyfuzz/tree/main/ultrajson/bug1
Status	**fixed, CVE assigned: CVE-2022-34074**
Issue	https://github.com/ultrajson/ultrajson/issues/537

Subject	Pyyaml
Vulnerability Type	Recursion error
Input	mutated seed by PolyFuzz

Description	RecursionError happened with specific inputs:
	
	Traceback (most recent call last):
	  File "/home/wen/git/polyfuzz/pyyaml/poc_load.py", line 10, in <module>
	  context = yaml.load(bytes, Loader=yaml.FullLoader)
	  File
	"/root/anaconda3/lib/python3.9/site-packages/PyYAML-6.0-py3.9-linux-x86_64.egg/yaml/__init__.py", line 81, in load
	  return loader.get_single_data()
	
	https://github.com/baltsers/polyfuzz/blob/main/pyyaml/pyyaml.log

PoC	https://github.com/baltsers/polyfuzz/tree/main/pyyaml
Status	pending
Issue	https://github.com/yaml/pyyaml/issues/642

Subject	Pillow
Vulnerability Type	Out of Memory
Input	mutated seed by PolyFuzz
Description	OOM happened with specific inputs:
PoC	https://github.com/baltsers/polyfuzz/tree/main/pillow

Status	**fixed, CVE assigned: CVE-2022-34075**
Issue	

Subject	Libsmbios
Vulnerability Type	segment fault
Input	mutated seed by PolyFuzz
Description	Segment fault happened with specific inputs: Program received signal SIGBUS, Bus error. __memmove_avx_unaligned_erms () at ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:283 283 ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S: No such file or directory. (gdb) bt #0 __memmove_avx_unaligned_erms () at ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:283 #1 0x00007ffff6bf01ac in memcpy (__len=1, __src=0x7ffff7e2f2f0, __dest=<optimized out>) at /usr/include/x86_64-linux-gnu/bits/string_fortified.h:34 #2 trycopy (rw=true, length=1, offset=<optimized out>, buffer=0x7ffff7e2f2f0 "a", private_data=0x555555a28640) at src/libsmbios_c/memory/memory_linux.c:141 #3 copy_mmap (this=0x5555559f82a0, buffer=0x7ffff7e2f2f0 "a", offset=0, length=1, rw=true) at src/libsmbios_c/memory/memory_linux.c:195 #4 0x00007ffff7fe29dd in ffi_call_unix64 () from /root/anaconda3/lib/python3.9/lib-dynload/../../libffi.so.7 #5 0x00007ffff7fe2067 in ffi_call_int () from /root/anaconda3/lib/python3.9/lib-dynload/../../libffi.so.7 #6 0x00007ffff7e200f6 in _call_function_pointer (argtypecount=<optimized out>,

	argcount=4, resmem=0x7fffffffd4d0, restype=<optimized out>, atypes=<optimized out>, avalues=<optimized out>, pProc=0x7ffff6bd17d0 <memory_obj_write>, flags=4353) at /usr/local/src/conda/python-3.9.7/Modules/_ctypes/callproc.c:920
PoC	https://github.com/baltsers/polyfuzz/tree/main/libsmbios
Status	pending
Issue	https://github.com/dell/libsmbios/issues/136

Subject	Javaparser
Vulnerability Type	JVM hangs
Input	mutated seed by PolyFuzz
Description	JVM hangs with specific inputs: Thread[main,5,main]at com.code_intelligence.jazzer.runtime.TraceDataFlowNativeCallbacks.traceCmpInt(Native Method)at com.code_intelligence.jazzer.runtime.TraceDataFlowNativeCallbacks.traceCmpInt(TraceDataFlowNativeCallbacks.java:47) https://github.com/baltsers/polyfuzz/blob/main/javaparser/javaparser.log
PoC	https://github.com/baltsers/polyfuzz/tree/main/javaparser
Status	CVE assigned:**CVE-2022-34073**
Issue	https://github.com/javaparser/javaparser/issues/3608

Subject	Jansi
Vulnerability Type	Out of Memory
Input	mutated seed by PolyFuzz
Description	OOM will happen with specific inputs: Exception in thread "main" java.lang.OutOfMemoryError: Java heap space at java.util.Arrays.copyOf(Arrays.java:3236) at java.io.ByteArrayOutputStream.grow(ByteArrayOutputStream.java:118)

	at java.io.ByteArrayOutputStream.ensureCapacity(ByteArrayOutputStream.java:93) at java.io.ByteArrayOutputStream.write(ByteArrayOutputStream.java:135) at org.fusesource.jansi.io.AnsiProcessor.processCursorDownLine(AnsiProcessor.java:517) at org.fusesource.jansi.io.AnsiProcessor.processEscapeCommand(AnsiProcessor.java:75) at org.fusesource.jansi.io.AnsiOutputStream.processEscapeCommand(AnsiOutputStream.java:304) at org.fusesource.jansi.io.AnsiOutputStream.write(AnsiOutputStream.java:204) at java.io.FilterOutputStream.write(FilterOutputStream.java:125) at java.io.FilterOutputStream.write(FilterOutputStream.java:97) at OsJansi.OutStream.main(OutStream.java:64)
PoC	https://github.com/baltsers/polyfuzz/tree/main/jansi
Status	CVE assigned:**CVE-2022-34072**
Issue	https://github.com/fusesource/jansi/issues/239

Subject	Aubio
Vulnerability Type	Memory leak
Input	mutated seed by PolyFuzz
Description	Memory will continue to grow with specific inputs: (base) root@ubuntu:/git/polyfuzz/aubio# ./run.sh case-abnormal [1] Thu May 19 23:31:13 PDT 2022: memory percentage: 0.1 [2] Thu May 19 23:31:43 PDT 2022: memory percentage: 1.9 [3] Thu May 19 23:32:13 PDT 2022: memory percentage: 3.0 [4] Thu May 19 23:32:43 PDT 2022: memory percentage: 4.1 [5] Thu May 19 23:33:13 PDT 2022: memory percentage: 5.2 [6] Thu May 19 23:33:43 PDT 2022: memory percentage: 6.3 [7] Thu May 19 23:34:13 PDT 2022: memory percentage: 7.4 [8] Thu May 19 23:34:43 PDT 2022: memory percentage: 8.5 [9] Thu May 19 23:35:13 PDT 2022: memory percentage: 9.6 [10] Thu May 19 23:35:43 PDT 2022: memory percentage: 10.6

PoC	https://github.com/baltsers/polyfuzz/tree/main/aubio
Status	pending
Issue	https://github.com/aubio/aubio/issues/363

Subject	Bottleneck.`median`
Vulnerability Type	Segment fault
Input	mutated seed by PolyFuzz

Description	Bottleneck.`nanmedian` `crashed with specific input`
	
	`Thread 1 "python" received signal SIGSEGV, Segmentation fault.`
	`0x00007fffd9ed80a0 in median_all_float64 (a=<optimized out>,`
	`ddof=<optimized out>) at bottleneck/src/reduce_template.c:822`
	`822 bottleneck/src/reduce_template.c: No such file or directory.`
	`(gdb) bt`
	`#0 0x00007fffd9ed80a0 in median_all_float64 (a=<optimized out>,`
	`ddof=<optimized out>) at bottleneck/src/reduce_template.c:822`
	`#1 0x00007fffd9ebb6cd in reducer (name=0x7fffd9ee29b4 "median",`
	`args=<optimized out>, args@entry=0x7ffff7f00a60, kwds=<optimized out>,`
	`kwds@entry=0x0,`
	`fall_float64=0x7fffd9ed7d40 <median_all_float64>,`
	`fall_float32=0x7fffd9ed8690 <median_all_float32>,`
	`fall_int64=0x7fffd9ed8fd0 <median_all_int64>,`
	`fall_int32=0x7fffd9ed98c0 <median_all_int32>,`
	`fone_float64=0x7fffd9eda2f0 <median_one_float64>,`
	`fone_float32=0x7fffd9edaff0 <median_one_float32>,`
	`fone_int64=0x7fffd9edbce0 <median_one_int64>,`
	`fone_int32=0x7fffd9edc950 <median_one_int32>, has_ddof=0) at`
	`bottleneck/src/reduce_template.c:1246`
	`#2 0x00007fffd9ebae5f in median (self=<optimized out>, args=0x0,`
	`kwds=0x2d) at bottleneck/src/reduce_template.c:892`
	`#3 0x00005555556c8714 in cfunction_call () at`
	`/tmp/build/80754af9/python-split_1631797238431/work/Objects/methodobje`
	`ct.c:543`

PoC	https://github.com/baltsers/polyfuzz/tree/main/bottleneck
Status	CVE assigned: **CVE-2022-34070**
Issue	https://github.com/pydata/bottleneck/issues/409

Subject	Bottleneck.nanmean
Vulnerability Type	Segment fault
Input	mutated seed by PolyFuzz
Description	Bottleneck.nanmean crashed with specific input Thread 1 "python" received signal SIGSEGV, Segmentation fault. nanmean_all_float64 (a=<optimized out>, ddof=<optimized out>) at bottleneck/src/reduce_template.c:169 169 bottleneck/src/reduce_template.c: No such file or directory. (gdb) bt #0 nanmean_all_float64 (a=<optimized out>, ddof=<optimized out>) at bottleneck/src/reduce_template.c:169 #1 0x00007fffd9ebb6cd in reducer (name=0x7fffd9ee2979 "nanmean", args=<optimized out>, args@entry=0x7ffff7f00a60, kwds=<optimized out>, kwds@entry=0x0, fall_float64=0x7fffd9ebeac0 <nanmean_all_float64>, fall_float32=0x7fffd9ebee50 <nanmean_all_float32>, fall_int64=0x7fffd9ebf1f0 <nanmean_all_int64>, fall_int32=0x7fffd9ebf670 <nanmean_all_int32>, fone_float64=0x7fffd9ebfa60 <nanmean_one_float64>, fone_float32=0x7fffd9ec0260 <nanmean_one_float32>, fone_int64=0x7fffd9ec0a40 <nanmean_one_int64>, fone_int32=0x7fffd9ec1350 <nanmean_one_int32>, has_ddof=0) at bottleneck/src/reduce_template.c:1246 #2 0x00007fffd9ebaa5f in nanmean (self=<optimized out>, args=0x0, kwds=0x2d) at bottleneck/src/reduce_template.c:259
PoC	https://github.com/baltsers/polyfuzz/tree/main/bottleneck
Status	CVE assigned: **CVE-2022-34070**
Issue	https://github.com/pydata/bottleneck/issues/409

Subject	Bottleneck.nanmedian
Vulnerability Type	Segment fault
Input	mutated seed by PolyFuzz
Description	Bottleneck.nanmedian crashed with specific input Thread 1 "python" received signal SIGSEGV, Segmentation fault. 0x00007fffd9edd9d0 in nanmedian_all_float64 (a=<optimized out>, ddof=<optimized out>) at bottleneck/src/reduce_template.c:822 822 bottleneck/src/reduce_template.c: No such file or directory. (gdb) bt #0 0x00007fffd9edd9d0 in nanmedian_all_float64 (a=<optimized out>, ddof=<optimized out>) at bottleneck/src/reduce_template.c:822

	#1 0x00007fffd9ebb6cd in reducer (name=0x7fffd9ee29bb "nanmedian", args=<optimized out>, args@entry=0x7ffff7f00a60, kwds=<optimized out>, kwds@entry=0x0,
	    fall_float64=0x7fffd9edd6f0 <nanmedian_all_float64>, fall_float32=0x7fffd9ede040 <nanmedian_all_float32>, fall_int64=0x7fffd9ed8fd0 <median_all_int64>,
	    fall_int32=0x7fffd9ed98c0 <median_all_int32>, fone_float64=0x7fffd9ede960 <nanmedian_one_float64>, fone_float32=0x7fffd9edf630 <nanmedian_one_float32>,
	    fone_int64=0x7fffd9edbce0 <median_one_int64>, fone_int32=0x7fffd9edc950 <median_one_int32>, has_ddof=0) at bottleneck/src/reduce_template.c:1246
	#2 0x00007fffd9ebaedf in nanmedian (self=<optimized out>, args=0x0, kwds=0x2d) at bottleneck/src/reduce_template.c:897

PoC	https://github.com/baltsers/polyfuzz/tree/main/bottleneck
Status	CVE assigned: **CVE-2022-34070**
Issue	https://github.com/pydata/bottleneck/issues/409

Subject	Bottleneck.nanstd
Vulnerability Type	Segment fault
Input	mutated seed by PolyFuzz

Description	Bottleneck.nanstd crashed with specific input
	
	Thread 1 "python" received signal SIGSEGV, Segmentation fault.
	nanstd_all_float64 (a=<optimized out>, ddof=0) at bottleneck/src/reduce_template.c:275
	275 bottleneck/src/reduce_template.c: No such file or directory.
	(gdb) bt
	#0 nanstd_all_float64 (a=<optimized out>, ddof=0) at bottleneck/src/reduce_template.c:275
	#1 0x00007fffd9ebb6cd in reducer (name=0x7fffd9ee2981 "nanstd", args=<optimized out>, args@entry=0x7ffff7f00a60, kwds=<optimized out>, kwds@entry=0x0,
	    fall_float64=0x7fffd9ec1ba0 <nanstd_all_float64>, fall_float32=0x7fffd9ec2350 <nanstd_all_float32>, fall_int64=0x7fffd9ec2ae0 <nanstd_all_int64>,
	    fall_int32=0x7fffd9ec3310 <nanstd_all_int32>, fone_float64=0x7fffd9ec3a60 <nanstd_one_float64>, fone_float32=0x7fffd9ec4500 <nanstd_one_float32>,
	    fone_int64=0x7fffd9ec4f70 <nanstd_one_int64>, fone_int32=0x7fffd9ec5aa0 <nanstd_one_int32>, has_ddof=1) at bottleneck/src/reduce_template.c:1246
	#2 0x00007fffd9ebaadf in nanstd (self=<optimized out>, args=0x0, kwds=0x2d) at bottleneck/src/reduce_template.c:408

PoC	https://github.com/baltsers/polyfuzz/tree/main/bottleneck
Status	CVE assigned: **CVE-2022-34070**

Issue	https://github.com/pydata/bottleneck/issues/409

Subject	Bottleneck.ss
Vulnerability Type	Segment fault
Input	mutated seed by PolyFuzz
Description	Bottleneck.ss crashed with specific input Thread 1 "python" received signal SIGSEGV, Segmentation fault. 0x00007fffd9ed5608 in ss_all_float64 (a=<optimized out>, ddof=<optimized out>) at bottleneck/src/reduce_template.c:661 661 bottleneck/src/reduce_template.c: No such file or directory. (gdb) bt #0 0x00007fffd9ed5608 in ss_all_float64 (a=<optimized out>, ddof=<optimized out>) at bottleneck/src/reduce_template.c:661 #1 0x00007fffd9ebb6cd in reducer (name=0x7fffd9ee29b1 "ss", args=<optimized out>, args@entry=0x7ffff7f00a60, kwds=<optimized out>, kwds@entry=0x0, fall_float64=0x7fffd9ed54a0 <ss_all_float64>, fall_float32=0x7fffd9ed58a0 <ss_all_float32>, fall_int64=0x7fffd9ed5ca0 <ss_all_int64>, fall_int32=0x7fffd9ed6090 <ss_all_int32>, fone_float64=0x7fffd9ed6440 <ss_one_float64>, fone_float32=0x7fffd9ed6ab0 <ss_one_float32>, fone_int64=0x7fffd9ed7130 <ss_one_int64>, fone_int32=0x7fffd9ed7770 <ss_one_int32>, has_ddof=0) at bottleneck/src/reduce_template.c:1246 #2 0x00007fffd9ebaddf in ss (self=<optimized out>, args=0x0, kwds=0x90) at bottleneck/src/reduce_template.c:729
PoC	https://github.com/baltsers/polyfuzz/tree/main/bottleneck
Status	CVE assigned: **CVE-2022-34070**
Issue	https://github.com/pydata/bottleneck/issues/409

Subject	Bottleneck.nanmin
Vulnerability Type	Segment fault
Input	mutated seed by PolyFuzz
Description	Bottleneck.nanmin crashed with specific input hread 1 "python" received signal SIGSEGV, Segmentation fault. nanmin_all_float64 (a=<optimized out>, ddof=<optimized out>) at bottleneck/src/reduce_template.c:432

	432 bottleneck/src/reduce_template.c: No such file or directory. (gdb) bt #0 nanmin_all_float64 (a=<optimized out>, ddof=<optimized out>) at bottleneck/src/reduce_template.c:432 #1 0x00007fffd9ebb6cd in reducer (name=0x7fffd9ee298f "nanmin", args=<optimized out>, args@entry=0x7ffff7f00a60, kwds=<optimized out>, kwds@entry=0x0, fall_float64=0x7fffd9ecae00 <nanmin_all_float64>, fall_float32=0x7fffd9ecb320 <nanmin_all_float32>, fall_int64=0x7fffd9ecb800 <nanmin_all_int64>, fall_int32=0x7fffd9ecbc20 <nanmin_all_int32>, fone_float64=0x7fffd9ecc020 <nanmin_one_float64>, fone_float32=0x7fffd9ecc700 <nanmin_one_float32>, fone_int64=0x7fffd9eccdb0 <nanmin_one_int64>, fone_int32=0x7fffd9ecd3c0 <nanmin_one_int32>, has_ddof=0) at bottleneck/src/reduce_template.c:1246 #2 0x00007fffd9ebabdf in nanmin (self=<optimized out>, args=0x0, kwds=0x95) at bottleneck/src/reduce_template.c:517
PoC	https://github.com/baltsers/polyfuzz/tree/main/bottleneck
Status	CVE assigned: **CVE-2022-34070**
Issue	https://github.com/pydata/bottleneck/issues/409

Subject	Bottleneck.nanmax
Vulnerability Type	Segment fault
Input	mutated seed by PolyFuzz
Description	Bottleneck.nanmax crashed with specific input Thread 1 "python" received signal SIGSEGV, Segmentation fault. nanmin_all_float64 (a=<optimized out>, ddof=<optimized out>) at bottleneck/src/reduce_template.c:432 432 bottleneck/src/reduce_template.c: No such file or directory. (gdb) bt #0 nanmin_all_float64 (a=<optimized out>, ddof=<optimized out>) at bottleneck/src/reduce_template.c:432 #1 0x00007fffd9ebb6cd in reducer (name=0x7fffd9ee298f "nanmin", args=<optimized out>, args@entry=0x7ffff7f00a60, kwds=<optimized out>, kwds@entry=0x0, fall_float64=0x7fffd9ecae00 <nanmin_all_float64>, fall_float32=0x7fffd9ecb320 <nanmin_all_float32>, fall_int64=0x7fffd9ecb800 <nanmin_all_int64>, fall_int32=0x7fffd9ecbc20 <nanmin_all_int32>, fone_float64=0x7fffd9ecc020 <nanmin_one_float64>, fone_float32=0x7fffd9ecc700 <nanmin_one_float32>, fone_int64=0x7fffd9eccdb0 <nanmin_one_int64>, fone_int32=0x7fffd9ecd3c0 <nanmin_one_int32>, has_ddof=0) at bottleneck/src/reduce_template.c:1246 #2 0x00007fffd9ebabdf in nanmax(self=<optimized out>, args=0x0, kwds=0x95) at bottleneck/src/reduce_template.c:517

PoC	https://github.com/baltsers/polyfuzz/tree/main/bottleneck
Status	CVE assigned: **CVE-2022-34070**
Issue	https://github.com/pydata/bottleneck/issues/409