Group-based Corpus Scheduling for Parallel Fuzzing

Anonymous Author(s)*

1 BUG LIST

Table 1: The vulnerabilities found by glibFuzzer.

Program	Type	Position	Status
php	heap-use-after-free	/src/php-src/Zend/zend_vm_execute.h:22878:3	fixed
php	memory leaks	/src/php-src/Zend/zend_vm_execute.h:47115:3	fixed
php	memory leaks	/src/php-src/Zend/zend_vm_execute.h:22037:3	fixed
php	memory leaks	/src/php-src/Zend/zend_vm_execute.h:17503:10	fixed
php	memory leaks	/src/php-src/Zend/zend_vm_execute.h:43340:3	fixed
php	memory leaks	/src/php-src/Zend/zend_vm_execute.h:46131:10	fixed
php	SEGV	/src/php-src/Zend/zend_types.h:1179:2	fixed
libraw	stack-buffer-overflow	/src/libraw/src/libraw_datastream.cpp:288	fixed
libraw	integer overflow	src/demosaic/misc_demosaic.cpp:92:20	reported
libraw	integer overflow	src/metadata/identify_tools.cpp:97:20	reported
nginx	SEGV	njs_vmcode_array /src/njs/src/njs_vmcode.c:1040:17	fixed
nginx	divide-by-zero	/src/njs_vmcode.c:414:25	fixed
libhevc	assertion failed	/src/libhevc/common/ihevc_buf_mgr.c:322	fixed
libarchive	SEGV	/src/libarchive/libarchive/archive_read_support_format_zip.c	fixed
bls-signature	assertion failed	/src/cryptofuzz/executor.cpp:1944:5	fixed
wireshark	SEGV	/src/wireshark/epan/tvbuff.c:827:3	fixed
wireshark	global-buffer-overflow	/src/wireshark/epan/dissectors/packet-ieee80211.c:11810:16	fixed
adobe dng_sdk	stack-buffer-overflow	/src/dng_sdk/source/./dng_info.cpp:184:7	fixed
C-Blosc2	heap-buffer-overflow	/src/c-blosc2/plugins/codecs/ndlz/ndlz8x8.c:457:3	fixed
C-Blosc2	SEGV	/src/c-blosc2/blosc/blosc2-stdio.c:47:21	fixed
dnsmasq	heap-buffer-overflow	/src/dnsmasq/src/rfc1035.c:106:11	fixed
dnsmasq	memory leaks	/src/dnsmasq/src/rfc2131.c:626:11	fixed
libass	use-of-uninitialized-value	/src/libass/libass/ass_fontconfig.c:333:10	fixed
libass	integer overflow	../../src/harfbuzz/src/hb-set-digest.hh:75:24	reported
libass	division by zero	ass_render.c:1857:26	reported
lzo	heap-buffer-overflow	/src/lzo-2.10/src/lzo1f_d.ch	fixed
lzo	use-of-uninitialized-value	/src/lzo-2.10/src/lzo1c_cc.c:72:13	fixed
lzo	use-of-uninitialized-value	/src/lzo-2.10/src/lzo1b_sm.ch:92:21	reported
json	stack-overflow	/src/json/single_include/nlohmann/json.hpp:9002:24	fixed
freeimage	use-of-uninitialized-value	/src/freeimage-svn/FreeImage/trunk/Source/FreeImage/PluginICO.cpp:202	fixed
freeimage	integer overflow	/src/freeimage-svn/FreeImage/trunk/Source/LibRawLite/src/metadata/hasselblad_model.cpp:92:23	fixed
cpython3	use-of-uninitialized-value	/src/cpython3/Objects/longobject.c:226:9	fixed
elfutils	memory leaks	/src/elfutils/libdwfl/dwfl_begin.c:44:16	fixed
elfutils	use-of-uninitialized-value	/src/elfutils/src/libreadelf.c:2888:7	fixed
geos	use-of-uninitialized-value	/src/geos/src/geomgraph/Node.cpp:163:1	fixed
geos	integer overflow	/src/geos/src/operation/overlay/ElevationMatrix.cpp:172:45	reported
gopacket	Slice bounds out of range	github.com/google/gopacket/layers/fuzz_layer.go:31	fixed
libcoap	use-of-unintialized-value	/src/libcoap/src/uri.c:72:7	fixed
fluent-bit	use-of-unintialized-value	/src/fluent-bit/src/flb_regex.c:48:34	fixed
fluent-bit	unknown read	/src/fluent-bit/lib/monkey/mk_core/mk_rconf.c:260:13	fixed
fluent-bit	memory leaks	/src/fluent-bit/lib/monkey/mk_core/mk_rconf.c:251:11	reported
gpac	use-of-unintialized-value	/src/gpac/src/isomedia/isom_intern.c:903:19	fixed
gpac	heap-buffer-overflow	/src/gpac/src/isomedia/box_code_base.c:5677:24	fixed
gpac	memory leaks	/src/gpac/src/isomedia/box_code_base.c:143:3	reported
go-sqlite3	use-of-unintialized-value	/_/github.com/mattn/go-sqlite3@/sqlite3-binding.c:31763:28	fixed
blackfriday	Index out of range	github.com/russross/blackfriday/render_fuzzer.go:19	fixed
hiredis	heap-double-free	/src/hiredis/alloc.h:79:5	fixed
hiredis	null-dereference READ	/src/hiredis/hiredis.c:364:24	fixed
hiredis	use-of-uninitialized-value	/src/hiredis/format_command_fuzzer.c:38	fixed
assimp	null-dereference READ	/src/assimp/code/AssetLib/X3D/X3DImporter.cpp:269:29	fixed
dropbear	use-of-unintialized-value	/src/dropbear/libtomcrypt/src/hashes/sha2/sha512.c:112:16	fixed
dropbear	global-buffer-overflow	/src/dropbear/fuzz/fuzz-wrapfd.c:62:2	fixed
htslib	use-of-unintialized-value	/src/htslib/htscodecs/htscodecs/tokenise_name3.c:1026:9	fixed
htslib	use-of-unintialized-value	/src/htslib/htscodecs/htscodecs/rANS_static4x16pr.c:1452:9	fixed
libpg_query	use-of-unintialized-value	/src/libpg_query/scan.l:1220:6	fixed
libpg_query	stack-overflow	/src/libpg_query/src/postgres/src_port_snprintf.c:1320:3	fixed
libpg_query	stack-overflow	/src/libraw/src/metadata/misc_parsers.cpp:311:16	reported
haproxy	null-dereference WRITE	/src/haproxy/src/arg.c:225:26	fixed
haproxy	Undefined-shift	/src/haproxy/src/hpack-huff.c:1457:55	fixed
haproxy	null-dereference	/src/haproxy/src/cfgparse.c:2134:3	reported
jsoncons	use-of-unintialized-value	/src/jsoncons/include/jsoncons_ext/cbor/cbor_parser.hpp:228:25	fixed
jsoncons	interger overflow	/src/jsoncons/include/jsoncons/bigint.hpp:899:31	fixed
libvpx	SEGV	/src/libvpx/vp8/decoder/detokenize.c:167:43	fixed
boost	integer overflow	/src/include/boost/regex/v5/basic_regex_creator.hpp	fixed
SerenityOS	bounds overflow	Userland/Libraries/LibGfx/JPGLoader.cpp:424	fixed
libgit2	undefined-behavior	/src/libgit2/src/midx.c:224:67	reported
espeak_ng	stack-buffer-overflow	/src/espeak-ng/src/libespeak-ng/numbers.c:1051:102	reported
espeak_ng	heap-buffer-overflow	/src/espeak-ng/src/libespeak-ng/encoding.c:539:15	reported
cfengine	stack-overflow	/src/core/libpromises/string_expressions.c:234:33	reported
exiv2	use-of-unintialized-value	/src/exiv2/src/basicio.cpp:1319:13	reported
libucl	heap-buffer-overflow	/src/libcoap/src/uri.c:72:7	reported
libsrtp	use-of-unintialized-value	/src/libsrtp/crypto/cipher/aes.c:1662:34	reported
libsrtp	heap-buffer-overflow	/src/libsrtp/srtp/srtp.c:965:5	reported
cppcheck	null-dereference READ	/src/cppcheck/lib/token.h:821:16	reported
cppcheck	undefined-behavior	/lib/checkunusedfunctions.cpp:225:36	reported
libheif	heap-buffer-overflow	libheif/heif_colorconversion.cc:529	fixed
libheif	use-of-unintialized-value	/src/libde265/libde265/fallback-dct.cc:401:25	reported
libheif	heap-buffer-overflow	/src/libde265/libde265/sao.cc:252:28	reported
libheif	memory leaks	/src/libheif/libheif/heif_encoder_x265.cc:895:22	reported
libheif	use-of-unintialized-value	/src/libde265/libde265/deblock.cc:542:15	reported
libheif	heap-buffer-overflow	/src/libheif/libheif/heif_colorconversion.cc:529:7	reported
libtsm	global-buffer-overflow READ	/src/libtsm/src/tsm/tsm-vte.c:514:8	reported
libtsm	memory leaks	/src/libtsm/src/tsm/tsm-screen.c:138:16	reported
libfido2	use-of-unintialized-value	/src/libfido2/src/netlink.c:0:10	reported

vlc	use-of-unintialized-value	/src/vlc/src/config/getopt.c:258:9	reported
vlc	assertion failed	/src/vlc/src/misc/mtime.c:91:5	reported
vlc	use-of-unintialized-value	/src/vlc/src/misc/block.c:122:18	reported
vlc	memory leaks	/src/vlc/modules/demux/mpeg/ps.h:310:32	reported
kamailio	unknown read	/src/kamailio/src/core/parser/parse_identityinfo.c:315:3	reported
gcloud	stack-overflow	cloud.google.com/go/spanner/spansql/parser.go:2487	reported
draco	invalid-enum-value	/src/draco/src/draco/compression/attributes/sequential_integer_attribute_decoder.cc:98:7	reported
duckdb	divide-by-zero	/src/duckdb/src/common/operator/cast_operators.cpp:1064:46	fixed
lcms	integer overflow	/src/lcms/src/cmsintrp.c:0	reported
libcbor	null-dereference	/src/libcbor/src/cbor/common.c:157:9	reported
libjxl	SEGV	/src/libjxl/third_party/highway/hwy/ops/x86_512-inl.h:1863:3	reported
libjxl	heap-buffer-overflow	/src/libjxl/lib/jxl/image_ops.h:55:5	reported
libjxl	integer overflow	/src/libjxl/lib/jxl/modular/encoding/dec_ma.cc:52:26	fixed
keystone	assertion failed	/src/keystone/llvm/lib/Target/Mips/AsmParser/MipsAsmParser.cpp:4773	reported
cctz	integer overflow	/src/cctz/include/cctz/time_zone.h:407:10	reported
libxls	use-of-unintialized-value	/src/libxls/src/ole.c:80:5	reported
libxls	use-of-unintialized-value	/src/libxls/src/ole.c:491:13	reported
go-ethereum	fatal error	_cgo_try_pthread_create /_/runtime/cgo/gcc_libinit.c:100:9	reported
gfwx	integer-overflow	/src/gfwx-fuzzers/decoder.cpp:38:108	reported
libpng-proto	memory leaks	/src/libpng/pngmem.c:95:17	reported
openjpeg	unsigned integer overflow	/src/openjpeg/src/lib/openjp2/opj_intmath.h:292:28	reported
xpdf	memory leaks	/src/xpdf-4.03/xpdf/PDFDoc.cc:216:9	reported
libssh	use-of-unintialized-value	/src/libssh/src/dh_crypto.c:77:30	reported
libssh	use-of-unintialized-value	/src/libssh/src/pki_crypto.c:0	reported
libssh	use-of-unintialized-value	/src/libssh/src/misc.c:1225:14	reported
libyaml	use-of-unintialized-value	/src/libyaml/src/emitter.c:1797:5	reported
wpantund	SEGV	/usr/include/boost/any.hpp:173:22	reported
hostap	use-of-unintialized-value	/src/hostap/src/common/sae.c:1912:6	reported
xercesc	integer overflow	xercesc/util/XMLString.hpp:1606:28	reported
fio	integer overflow	parse.c:821:32	reported
libmpeg2	integer overflow	/src/libmpeg2/decoder/impeg2d_mv_dec.c:144:41	reported