Fuzzing Samba: how is it going?

Douglas Bagnall

dbagnall@samba.org

douglas.bagnall@catalyst.net.nz

Fuzzing recap

testing a program with random input

Fuzzing recap

testing a program with random input

or with evolving input

Fuzzing recap

testing a program with random input

“blackbox” fuzzing

or with evolving input

“coverage based” fuzzing

Fuzzing recap

testing a program with random input

“blackbox” fuzzing

or with evolving input

“coverage based” fuzzing

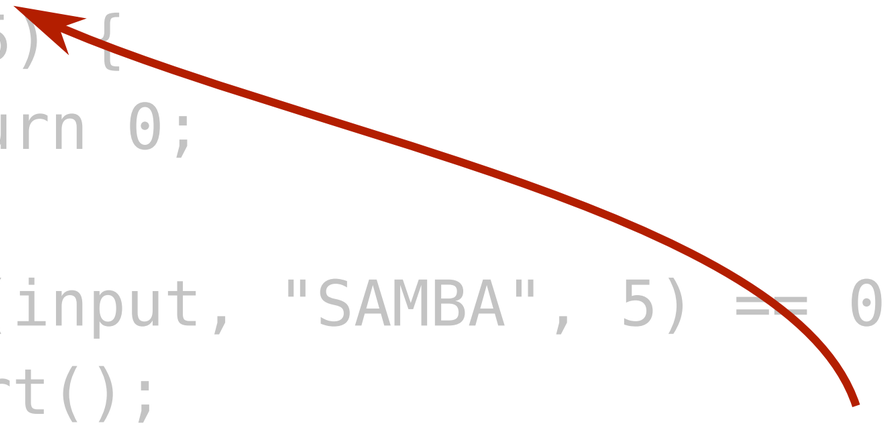
coverage based fuzzing needs a co-operative compiler, runtime, or CPU

a function that might crash

```
int test(char *input, size_t len) {
        if (len != 5) {
                return 0;
        }
        if (strncmp(input, "SAMBA", 5) == 0) {
                abort();
        }
        return 0;
}
```

a function that might crash

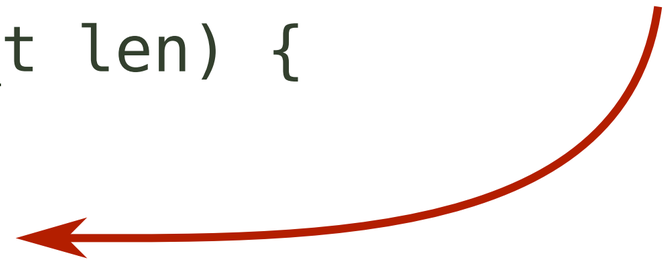
```
int test(char *input, size_t len) {
        if (len != 5) {
                return 0;
        }
        if (strncmp(input, "SAMBA", 5) == 0) {
                abort();
        }
        return 0;
}
```



takes a string and length,
returns nothing

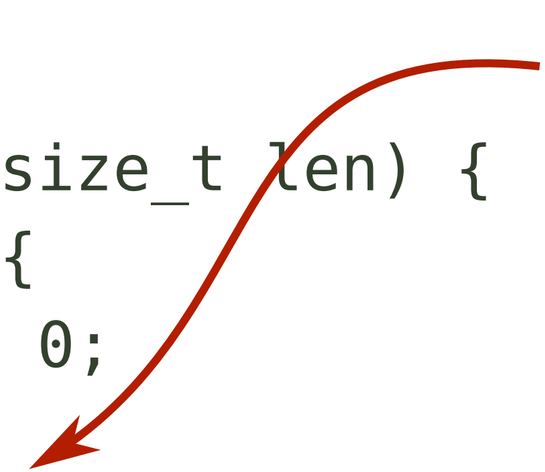
a function that might crash

if the length is not 5, do nothing



```
int test(char *input, size_t len) {
        if (len != 5) {
                return 0;
        }
        if (strncmp(input, "SAMBA", 5) == 0) {
                abort();
        }
        return 0;
}
```

a function that might crash



if the string is “SAMBA”,

…

```
int test(char *input, size_t len) {
        if (len != 5) {
                return 0;
        }
        if (strncmp(input, "SAMBA", 5) == 0) {
                abort();
        }
        return 0;
}
```

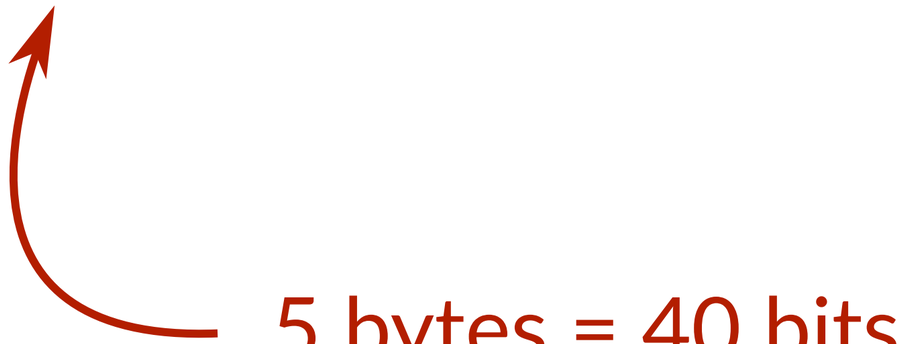
a function that might crash

```
int test(char *input, size_t len) {
        if (len != 5) {
                return 0;
        }
        if (strncmp(input, "SAMBA", 5) == 0) {
                abort();
        }
        return 0;
}
```

if the string is “SAMBA”, crash

a function that might crash: old-style fuzzing

```
int test(char *input, size_t len) {
        if (len != 5) {
                return 0;
        }
        if (strncmp(input, "SAMBA", 5) == 0) {
                abort();
        }
        return 0;
}
```



a function that might crash: old-style fuzzing

```
int test(char *input, size_t len) {
        if (len != 5) {
                return 0;
        }
        if (strncmp(input, "SAMBA", 5) == 0) {
                abort();
        }
        return 0;
}
```

chance of the length being 5?

a function that might crash: old-style fuzzing

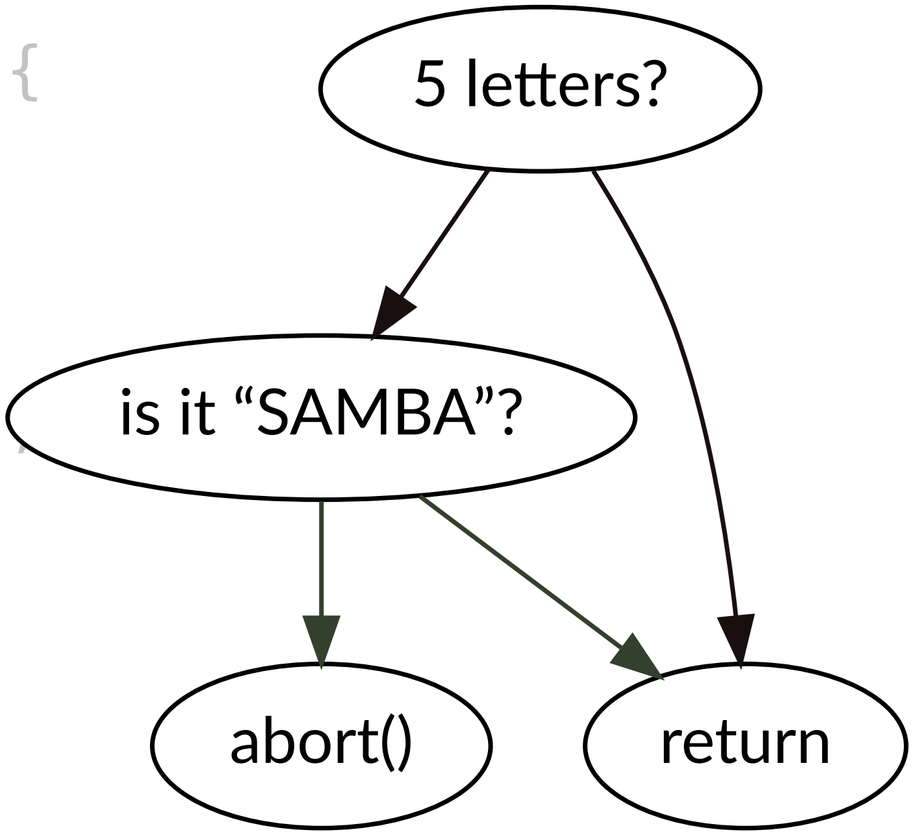
```
int test(char *input, size_t len) {
        if (len != 5) {
                return 0;
        }
        if (strncmp(input, "SAMBA", 5) == 0) {
                abort();
        }
        return 0;
}
```

1 in 1,000,000,000,000 × ε

chance of finding the crash

a function that might crash: coverage based fuzzing

```
int test(char *input, size_t len) {
        if (len != 5) {
                return 0;
        }
        if (strncmp(input, "SAMBA",
                abort();
        }
        return 0;
}
```



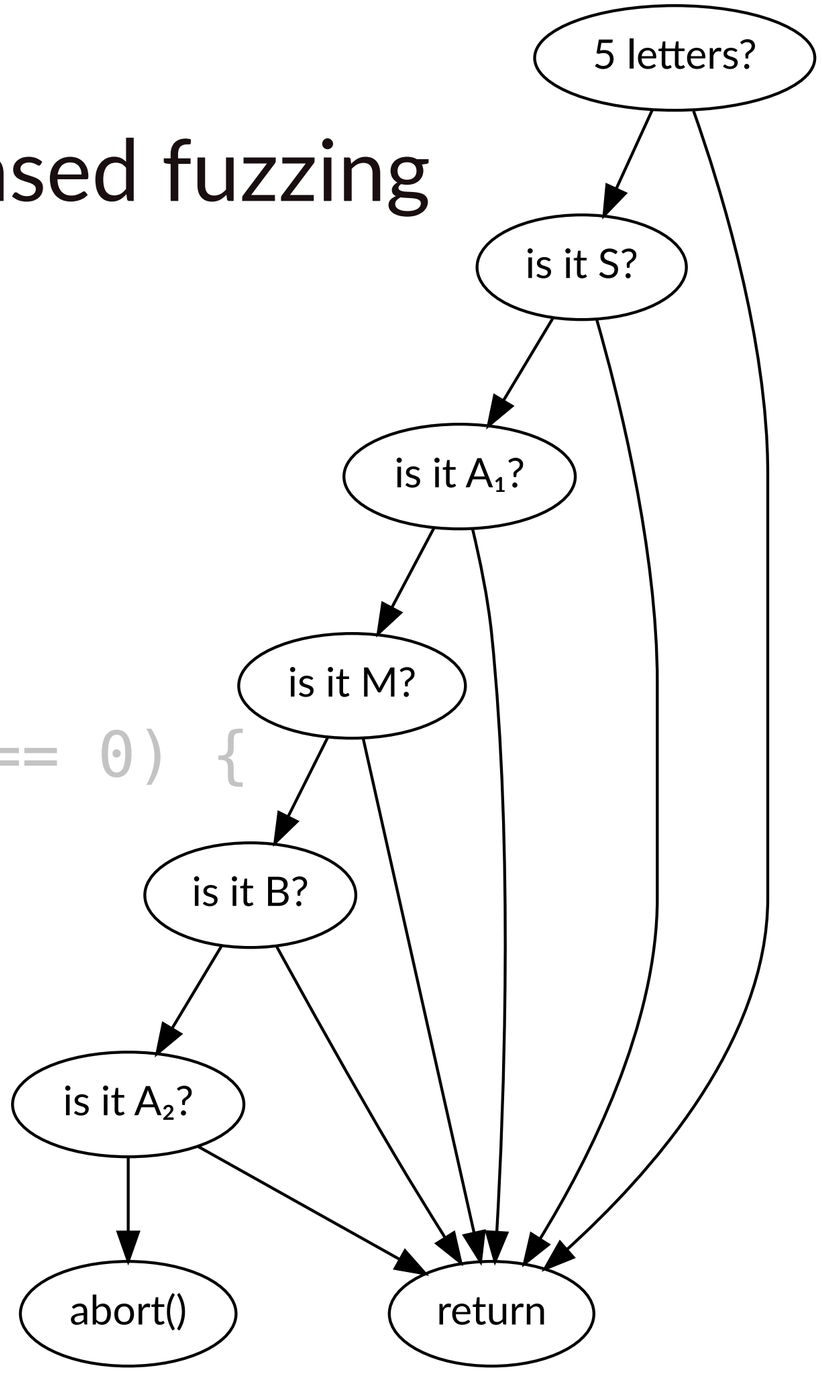
mutate and reproduce

inputs that cover new ground

a function that might crash: coverage based fuzzing

```
int test(char *input, size_t len) {
        if (len != 5) {
                return 0;
        }
        if (strncmp(input, "SAMBA", 5) == 0) {
                abort();
        }
        return 0;
}
```

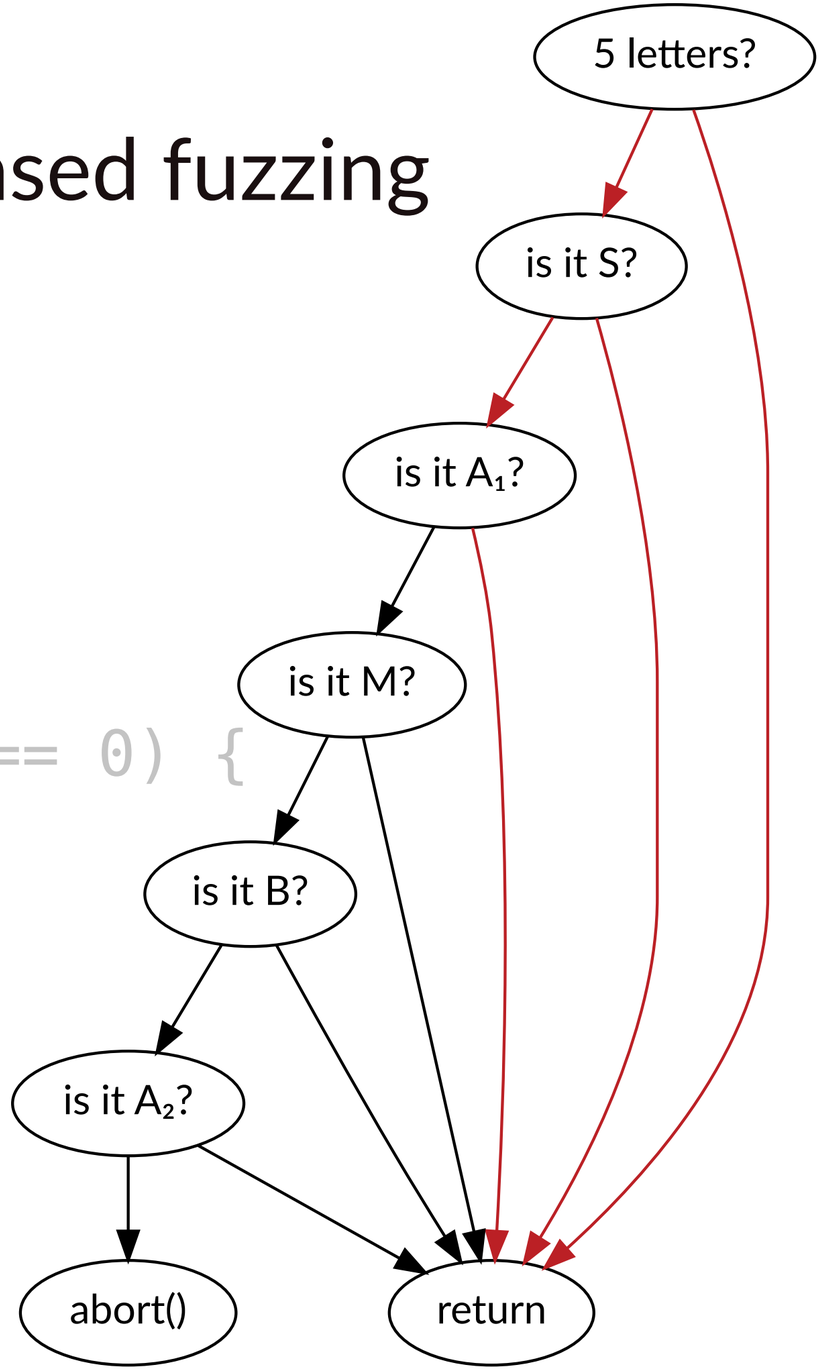
in the order of 5×256 + ε



a function that might crash: coverage based fuzzing

```
int test(char *input, size_t len) {
        if (len != 5) {
                return 0;
        }
        if (strncmp(input, "SAMBA", 5) == 0) {
                abort();
        }
        return 0;
}
```

in the order of 5×256 + ε



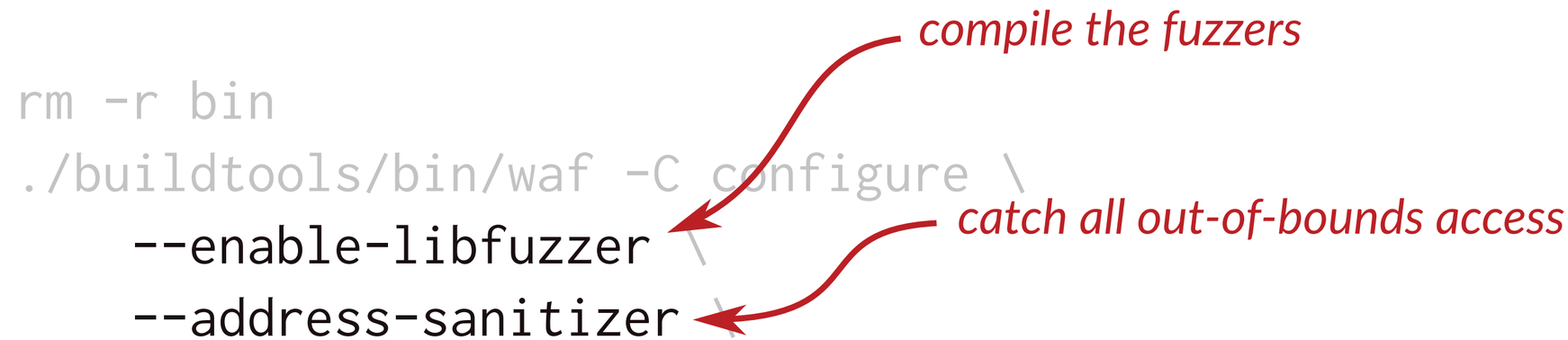
Fuzzing Samba recap

```
rm -r bin
./buildtools/bin/waf -C configure \
    --enable-libfuzzer \
    --address-sanitizer \
    CC=~/honggfuzz/hfuzz_cc/hfuzz-clang \
    LINK_CC=~/honggfuzz/hfuzz_cc/hfuzz-clang \
    --disable-warnings-as-errors \
    --abi-check-disable  \
    --without-gettext

make -j
```

Fuzzing Samba recap

Fuzzing Samba recap




```
rm -r bin
./buildtools/bin/waf -C configure \
    --enable-libfuzzer \
    --address-sanitizer \
    CC=~/honggfuzz/hfuzz_cc/hfuzz-clang \
    LINK_CC=~/honggfuzz/hfuzz_cc/hfuzz-clang \
    --disable-warnings-as-errors \
    --abi-check-disable  \
    --without-gettext

make -j
```

Fuzzing Samba recap

```
rm -r bin
./buildtools/bin/waf -C configure \
    --enable-libfuzzer \
    --address-sanitizer \
    CC=~/honggfuzz/hfuzz_cc/hfuzz-clang \
    LINK_CC=~/honggfuzz/hfuzz_cc/hfuzz-clang \
    --disable-warnings-as-errors \
    --abi-check-disable  \
    --without-gettext

make -j
```

compile the fuzzers

catch all out-of-bounds access

use a fuzzing compiler
(there are other ways)

Fuzzing Samba recap

```
rm -r bin
./buildtools/bin/waf -C configure \
    --enable-libfuzzer \
    --address-sanitizer \
    CC=~/honggfuzz/hfuzz_cc/hfuzz-clang \
    LINK_CC=~/honggfuzz/hfuzz_cc/hfuzz-clang \
    --disable-warnings-as-errors \
    --abi-check-disable  \
    --without-gettext

make -j
```

compile the fuzzers

catch all out-of-bounds access

use a fuzzing compiler
(there are other ways)

disable unhelpful stuff

Fuzzing Samba recap

```
echo 'hi' | bin/fuzz_regfio
bin/fuzz_regfio path/to/file

~/honggfuzz/honggfuzz -P \
  $MANY_MORE_OPTIONS -- \
  ./bin/fuzz_regfio
```

test a particular string

really run the fuzzer, using coverage based evolution.

Fuzzing Samba recap: OSS-Fuzz

OSS-Fuzz (Google) runs our fuzzers continuously
(or continuously-ish).

They send us reports with 90 day disclosure deadlines

The reports link to stack traces and fuzz strings

OSS-Fuzz

122 public reports

13 still open

OSS-Fuzz

122 public reports

13 still open

some newer reports, still under 90 day embargo

OSS-Fuzz

122 public reports

13 still open

some newer reports, still under 90 day embargo

nobody looks much

oss-fuzz oss-fuzz New issue Open issues label:Proj-samba Sign in

1 - 13 of 13 List Grid Chart

ID	Type	Component	Status	Proj	Reported	Owner	Summary + Labels
20419	Bug	----	New	samba	2020-01-29	----	samba:fuzz_ndr_drsuapi_TYPE_OUT: Stack-overflow with empty stacktrace ClusterFuzz Reproducible
38457	Bug	----	New	samba	2021-09-11	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Pointer-overflow in ndr_push___spoolss_EnumPrinterDataEx ClusterFuzz Unreproducible
38480	Bug-Security	----	New	samba	2021-09-11	----	samba:fuzz_ndr_nbt_TYPE_STRUCT: Heap-buffer-overflow in ndr_push_array_uint8 ClusterFuzz Unreproducible
38575	Bug	----	New	samba	2021-09-12	----	samba:fuzz_regfio: Timeout in fuzz_regfio ClusterFuzz Reproducible
38810	Bug	----	New	samba	2021-09-16	----	samba:fuzz_ndr_dnsserver_TYPE_STRUCT: Timeout in fuzz_ndr_dnsserver_TYPE_STRUCT ClusterFuzz Reproducible
48183	Bug	----	New	samba	2022-06-22	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Null-dereference READ in ndr_push_spoolss_PrinterEnumValues ClusterFuzz Unreproducible
48234	Bug	----	New	samba	2022-06-23	----	samba:fuzz_ndr_dfsblobs_TYPE_STRUCT: Out-of-memory in fuzz_ndr_dfsblobs_TYPE_STRUCT ClusterFuzz Reproducible
48328	Bug	----	New	samba	2022-06-24	----	samba:fuzz_ldb_parse_tree: Timeout in fuzz_ldb_parse_tree ClusterFuzz Reproducible
48808	Bug	----	New	samba	2022-07-06	----	samba:fuzz_ndr_bkupblobs_TYPE_STRUCT: Timeout in fuzz_ndr_bkupblobs_TYPE_STRUCT ClusterFuzz Reproducible
50597	Bug	----	New	samba	2022-08-24	----	samba:fuzz_ndr_ioxidresolver: Timeout in fuzz_ndr_ioxidresolver ClusterFuzz Reproducible
50927	Bug	----	New	samba	2022-09-02	----	samba:fuzz_ndr_preg_TYPE_STRUCT: Timeout in fuzz_ndr_preg_TYPE_STRUCT ClusterFuzz Reproducible
53748	Bug	----	New	samba	2022-11-25	----	samba:fuzz_ndr_drsblobs_TYPE_STRUCT: Timeout in fuzz_ndr_drsblobs_TYPE_STRUCT ClusterFuzz Reproducible
53838	Bug	----	New	samba	2022-11-28	----	samba:fuzz_parse_lpq_entry: Integer-overflow in parse_lpq_entry ClusterFuzz Reproducible

https://bugs.chromium.org/p/oss-fuzz/issues/list?q=label:Proj-samba

oss-fuzz oss-fuzz New issue Open issues label:Proj-samba Sign in

1 - 13 of 13 List Grid Chart

ID	Type	Component	Status	Proj	Reported	Owner	Summary + Labels
20419	Bug	----	New	samba	2020-01-29	----	samba:fuzz_ndr_drsuapi_TYPE_OUT: Stack-overflow with empty stacktrace ClusterFuzz Reproducible
38457	Bug	----	New	samba	2021-09-11	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Pointer-overflow in ndr_push___spoolss_EnumPrinterDataEx ClusterFuzz Unreproducible
38480	Bug-Security	----	New	samba	2021-09-11	----	samba:fuzz_ndr_nbt_TYPE_STRUCT: Heap-buffer-overflow in ndr_push_array_uint8 ClusterFuzz Unreproducible
38575	Bug	----	New	samba	2021-09-12	----	samba:fuzz_regfio: Timeout in fuzz_regfio ClusterFuzz Reproducible
38810	Bug	----	New	samba	2021-09-16	----	samba:fuzz_ndr_dnsserver_TYPE_STRUCT: Timeout in fuzz_ndr_dnsserver_TYPE_STRUCT ClusterFuzz Reproducible
48183	Bug	----	New	samba	2022-06-22	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Null-dereference READ in ndr_push_spoolss_PrinterEnumValues ClusterFuzz Unreproducible
48234	Bug	----	New	samba	2022-06-23	----	samba:fuzz_ndr_dfsblobs_TYPE_STRUCT: Out-of-memory in fuzz_ndr_dfsblobs_TYPE_STRUCT ClusterFuzz Reproducible
48328	Bug	----	New	samba	2022-06-24	----	samba:fuzz_ldb_parse_tree: Timeout in fuzz_ldb_parse_tree ClusterFuzz Reproducible
48808	Bug	----	New	samba	2022-07-06	----	samba:fuzz_ndr_bkupblobs_TYPE_STRUCT: Timeout in fuzz_ndr_bkupblobs_TYPE_STRUCT ClusterFuzz Reproducible
50597	Bug	----	New	samba	2022-08-24	----	samba:fuzz_ndr_ioxidresolver: Timeout in fuzz_ndr_ioxidresolver ClusterFuzz Reproducible
50927	Bug	----	New	samba	2022-09-02	----	samba:fuzz_ndr_preg_TYPE_STRUCT: Timeout in fuzz_ndr_preg_TYPE_STRUCT ClusterFuzz Reproducible
53748	Bug	----	New	samba	2022-11-25	----	samba:fuzz_ndr_drsblobs_TYPE_STRUCT: Timeout in fuzz_ndr_drsblobs_TYPE_STRUCT ClusterFuzz Reproducible
53838	Bug	----	New	samba	2022-11-28	----	samba:fuzz_parse_lpq_entry: Integer-overflow in parse_lpq_entry ClusterFuzz Reproducible

https://bugs.chromium.org/p/oss-fuzz/issues/list?q=label:Proj-samba

oss-fuzz oss-fuzz New issue Open issues label:Proj-samba Sign in

1 - 13 of 13 List Grid Chart

ID	Type	Component	Status	Proj	Reported	Owner	Summary + Labels
20419	Bug	----	New	samba	2020-01-29	----	samba:fuzz_ndr_drsuapi_TYPE_OUT: Stack-overflow with empty stacktrace ClusterFuzz Reproducible
38457	Bug	----	New	samba	2021-09-11	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Pointer-overflow in ndr_push___spoolss_EnumPrinterDataEx ClusterFuzz Unreproducible
38480	Bug-Security	----	New	samba	2021-09-11	----	samba:fuzz_ndr_nbt_TYPE_STRUCT: Heap-buffer-overflow in ndr_push_array_uint8 ClusterFuzz Unreproducible
38575	Bug	----	New	samba	2021-09-12	----	samba:fuzz_regfio: Timeout in fuzz_regfio ClusterFuzz Reproducible
38810	Bug	----	New	samba	2021-09-16	----	samba:fuzz_ndr_dnsserver_TYPE_STRUCT: Timeout in fuzz_ndr_dnsserver_TYPE_STRUCT ClusterFuzz Reproducible
48183	Bug	----	New	samba	2022-06-22	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Null-dereference READ in ndr_push_spoolss_PrinterEnumValues ClusterFuzz Unreproducible
48234	Bug	----	New	samba	2022-06-23	----	samba:fuzz_ndr_dfsblobs_TYPE_STRUCT: Out-of-memory in fuzz_ndr_dfsblobs_TYPE_STRUCT ClusterFuzz Reproducible
48328	Bug	----	New	samba	2022-06-24	----	samba:fuzz_ldb_parse_tree: Timeout in fuzz_ldb_parse_tree ClusterFuzz Reproducible
48808	Bug	----	New	samba	2022-07-06	----	samba:fuzz_ndr_bkupblobs_TYPE_STRUCT: Timeout in fuzz_ndr_bkupblobs_TYPE_STRUCT ClusterFuzz Reproducible
50597	Bug	----	New	samba	2022-08-24	----	samba:fuzz_ndr_ioxidresolver: Timeout in fuzz_ndr_ioxidresolver ClusterFuzz Reproducible
50927	Bug	----	New	samba	2022-09-02	----	samba:fuzz_ndr_preg_TYPE_STRUCT: Timeout in fuzz_ndr_preg_TYPE_STRUCT ClusterFuzz Reproducible
53748	Bug	----	New	samba	2022-11-25	----	samba:fuzz_ndr_drsblobs_TYPE_STRUCT: Timeout in fuzz_ndr_drsblobs_TYPE_STRUCT ClusterFuzz Reproducible
53838	Bug	----	New	samba	2022-11-28	----	samba:fuzz_parse_lpq_entry: Integer-overflow in parse_lpq_entry ClusterFuzz Reproducible

7/13 timeouts

oss-fuzz oss-fuzz New issue Open issues label:Proj-samba Sign in

1 - 13 of 13 List Grid Chart

ID	Type	Component	Status	Proj	Reported	Owner	Summary + Labels
20419	Bug	----	New	samba	2020-01-29	----	samba:fuzz_ndr_drsuapi_TYPE_OUT: Stack-overflow with empty stacktrace ClusterFuzz Reproducible
38457	Bug	----	New	samba	2021-09-11	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Pointer-overflow in ndr_push___spoolss_EnumPrinterDataEx ClusterFuzz Unreproducible
38480	Bug-Security	----	New	samba	2021-09-11	----	samba:fuzz_ndr_nbt_TYPE_STRUCT: Heap-buffer-overflow in ndr_push_array_uint8 ClusterFuzz Unreproducible
38575	Bug	----	New	samba	2021-09-12	----	samba:fuzz_regfio: Timeout in fuzz_regfio ClusterFuzz Reproducible
38810	Bug	----	New	samba	2021-09-16	----	samba:fuzz_ndr_dnsserver_TYPE_STRUCT: Timeout in fuzz_ndr_dnsserver_TYPE_STRUCT ClusterFuzz Reproducible
48183	Bug	----	New	samba	2022-06-22	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Null-dereference READ in ndr_push_spoolss_PrinterEnumValues ClusterFuzz Unreproducible
48234	Bug	----	New	samba	2022-06-23	----	samba:fuzz_ndr_dfsblobs_TYPE_STRUCT: Out-of-memory in fuzz_ndr_dfsblobs_TYPE_STRUCT ClusterFuzz Reproducible
48328	Bug	----	New	samba	2022-06-24	----	samba:fuzz_ldb_parse_tree: Timeout in fuzz_ldb_parse_tree ClusterFuzz Reproducible
48808	Bug	----	New	samba	2022-07-06	----	samba:fuzz_ndr_bkupblobs_TYPE_STRUCT: Timeout in fuzz_ndr_bkupblobs_TYPE_STRUCT ClusterFuzz Reproducible
50597	Bug	----	New	samba	2022-08-24	----	samba:fuzz_ndr_ioxidresolver: Timeout in fuzz_ndr_ioxidresolver ClusterFuzz Reproducible
50927	Bug	----	New	samba	2022-09-02	----	samba:fuzz_ndr_preg_TYPE_STRUCT: Timeout in fuzz_ndr_preg_TYPE_STRUCT ClusterFuzz Reproducible
53748	Bug	----	New	samba	2022-11-25	----	samba:fuzz_ndr_drsblobs_TYPE_STRUCT: Timeout in fuzz_ndr_drsblobs_TYPE_STRUCT ClusterFuzz Reproducible
53838	Bug	----	New	samba	2022-11-28	----	samba:fuzz_parse_lpq_entry: Integer-overflow in parse_lpq_entry ClusterFuzz Reproducible

1/13 insufficient memory on the fuzz machine

oss-fuzz oss-fuzz New issue Open issues label:Proj-samba Sign in

1 - 13 of 13 List Grid Chart

ID	Type	Component	Status	Proj	Reported	Owner	Summary + Labels
20419	Bug	----	New	samba	2020-01-29	----	samba:fuzz_ndr_drsuapi_TYPE_OUT: Stack-overflow with empty stacktrace ClusterFuzz Reproducible
38457	Bug	----	New	samba	2021-09-11	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Pointer-overflow in ndr_push___spoolss_EnumPrinterDataEx ClusterFuzz Unreproducible
38480	Bug-Security	----	New	samba	2021-09-11	----	samba:fuzz_ndr_nbt_TYPE_STRUCT: Heap-buffer-overflow in ndr_push_array_uint8 ClusterFuzz Unreproducible
38575	Bug	----	New	samba	2021-09-12	----	samba:fuzz_regfio: Timeout in fuzz_regfio ClusterFuzz Reproducible
38810	Bug	----	New	samba	2021-09-16	----	samba:fuzz_ndr_dnsserver_TYPE_STRUCT: Timeout in fuzz_ndr_dnsserver_TYPE_STRUCT ClusterFuzz Reproducible
48183	Bug	----	New	samba	2022-06-22	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Null-dereference READ in ndr_push_spoolss_PrinterEnumValues ClusterFuzz Unreproducible
48234	Bug	----	New	samba	2022-06-23	----	samba:fuzz_ndr_dfsblobs_TYPE_STRUCT: Out-of-memory in fuzz_ndr_dfsblobs_TYPE_STRUCT ClusterFuzz Reproducible
48328	Bug	----	New	samba	2022-06-24	----	samba:fuzz_ldb_parse_tree: Timeout in fuzz_ldb_parse_tree ClusterFuzz Reproducible
48808	Bug	----	New	samba	2022-07-06	----	samba:fuzz_ndr_bkupblobs_TYPE_STRUCT: Timeout in fuzz_ndr_bkupblobs_TYPE_STRUCT ClusterFuzz Reproducible
50597	Bug	----	New	samba	2022-08-24	----	samba:fuzz_ndr_ioxidresolver: Timeout in fuzz_ndr_ioxidresolver ClusterFuzz Reproducible
50927	Bug	----	New	samba	2022-09-02	----	samba:fuzz_ndr_preg_TYPE_STRUCT: Timeout in fuzz_ndr_preg_TYPE_STRUCT ClusterFuzz Reproducible
53748	Bug	----	New	samba	2022-11-25	----	samba:fuzz_ndr_drsblobs_TYPE_STRUCT: Timeout in fuzz_ndr_drsblobs_TYPE_STRUCT ClusterFuzz Reproducible
53838	Bug	----	New	samba	2022-11-28	----	samba:fuzz_parse_lpq_entry: Integer-overflow in parse_lpq_entry ClusterFuzz Reproducible

1/13 bug parsing lpq system info

oss-fuzz oss-fuzz New issue Open issues label:Proj-samba Sign in

1 - 13 of 13 List Grid Chart

ID	Type	Component	Status	Proj	Reported	Owner	Summary + Labels
20419	Bug	----	New	samba	2020-01-29	----	samba:fuzz_ndr_drsuapi_TYPE_OUT: Stack-overflow with empty stacktrace ClusterFuzz Reproducible
38457	Bug	----	New	samba	2021-09-11	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Pointer-overflow in ndr_push___spoolss_EnumPrinterDataEx ClusterFuzz Unreproducible
38480	Bug-Security	----	New	samba	2021-09-11	----	samba:fuzz_ndr_nbt_TYPE_STRUCT: Heap-buffer-overflow in ndr_push_array_uint8 ClusterFuzz Unreproducible
38575	Bug	----	New	samba	2021-09-12	----	samba:fuzz_regfio: Timeout in fuzz_regfio ClusterFuzz Reproducible
38810	Bug	----	New	samba	2021-09-16	----	samba:fuzz_ndr_dnsserver_TYPE_STRUCT: Timeout in fuzz_ndr_dnsserver_TYPE_STRUCT ClusterFuzz Reproducible
48183	Bug	----	New	samba	2022-06-22	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Null-dereference READ in ndr_push_spoolss_PrinterEnumValues ClusterFuzz Unreproducible
48234	Bug	----	New	samba	2022-06-23	----	samba:fuzz_ndr_dfsblobs_TYPE_STRUCT: Out-of-memory in fuzz_ndr_dfsblobs_TYPE_STRUCT ClusterFuzz Reproducible
48328	Bug	----	New	samba	2022-06-24	----	samba:fuzz_ldb_parse_tree: Timeout in fuzz_ldb_parse_tree ClusterFuzz Reproducible
48808	Bug	----	New	samba	2022-07-06	----	samba:fuzz_ndr_bkupblobs_TYPE_STRUCT: Timeout in fuzz_ndr_bkupblobs_TYPE_STRUCT ClusterFuzz Reproducible
50597	Bug	----	New	samba	2022-08-24	----	samba:fuzz_ndr_ioxidresolver: Timeout in fuzz_ndr_ioxidresolver ClusterFuzz Reproducible
50927	Bug	----	New	samba	2022-09-02	----	samba:fuzz_ndr_preg_TYPE_STRUCT: Timeout in fuzz_ndr_preg_TYPE_STRUCT ClusterFuzz Reproducible
53748	Bug	----	New	samba	2022-11-25	----	samba:fuzz_ndr_drsblobs_TYPE_STRUCT: Timeout in fuzz_ndr_drsblobs_TYPE_STRUCT ClusterFuzz Reproducible
53838	Bug	----	New	samba	2022-11-28	----	samba:fuzz_parse_lpq_entry: Integer-overflow in parse_lpq_entry ClusterFuzz Reproducible

2/13 unused? spoolss things

oss-fuzz oss-fuzz New issue Open issues label:Proj-samba Sign in

1 - 13 of 13 List Grid Chart

ID	Type	Component	Status	Proj	Reported	Owner	Summary + Labels
20419	Bug	----	New	samba	2020-01-29	----	samba:fuzz_ndr_drsuapi_TYPE_OUT: Stack-overflow with empty stacktrace ClusterFuzz Reproducible
38457	Bug	----	New	samba	2021-09-11	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Pointer-overflow in ndr_push___spoolss_EnumPrinterDataEx ClusterFuzz Unreproducible
38480	Bug-Security	----	New	samba	2021-09-11	----	samba:fuzz_ndr_nbt_TYPE_STRUCT: Heap-buffer-overflow in ndr_push_array_uint8 ClusterFuzz Unreproducible
38575	Bug	----	New	samba	2021-09-12	----	samba:fuzz_regfio: Timeout in fuzz_regfio ClusterFuzz Reproducible
38810	Bug	----	New	samba	2021-09-16	----	samba:fuzz_ndr_dnsserver_TYPE_STRUCT: Timeout in fuzz_ndr_dnsserver_TYPE_STRUCT ClusterFuzz Reproducible
48183	Bug	----	New	samba	2022-06-22	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Null-dereference READ in ndr_push_spoolss_PrinterEnumValues ClusterFuzz Unreproducible
48234	Bug	----	New	samba	2022-06-23	----	samba:fuzz_ndr_dfsblobs_TYPE_STRUCT: Out-of-memory in fuzz_ndr_dfsblobs_TYPE_STRUCT ClusterFuzz Reproducible
48328	Bug	----	New	samba	2022-06-24	----	samba:fuzz_ldb_parse_tree: Timeout in fuzz_ldb_parse_tree ClusterFuzz Reproducible
48808	Bug	----	New	samba	2022-07-06	----	samba:fuzz_ndr_bkupblobs_TYPE_STRUCT: Timeout in fuzz_ndr_bkupblobs_TYPE_STRUCT ClusterFuzz Reproducible
50597	Bug	----	New	samba	2022-08-24	----	samba:fuzz_ndr_ioxidresolver: Timeout in fuzz_ndr_ioxidresolver ClusterFuzz Reproducible
50927	Bug	----	New	samba	2022-09-02	----	samba:fuzz_ndr_preg_TYPE_STRUCT: Timeout in fuzz_ndr_preg_TYPE_STRUCT ClusterFuzz Reproducible
53748	Bug	----	New	samba	2022-11-25	----	samba:fuzz_ndr_drsblobs_TYPE_STRUCT: Timeout in fuzz_ndr_drsblobs_TYPE_STRUCT ClusterFuzz Reproducible
53838	Bug	----	New	samba	2022-11-28	----	samba:fuzz_parse_lpq_entry: Integer-overflow in parse_lpq_entry ClusterFuzz Reproducible

1/13 insufficient stack on the fuzz machine

oss-fuzz oss-fuzz New issue Open issues label:Proj-samba Sign in

1 - 13 of 13 List Grid Chart

ID	Type	Component	Status	Proj	Reported	Owner	Summary + Labels
20419	Bug	----	New	samba	2020-01-29	----	samba:fuzz_ndr_drsuapi_TYPE_OUT: Stack-overflow with empty stacktrace ClusterFuzz Reproducible
38457	Bug	----	New	samba	2021-09-11	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Pointer-overflow in ndr_push___spoolss_EnumPrinterDataEx ClusterFuzz Unreproducible
38480	Bug-Security	----	New	samba	2021-09-11	----	samba:fuzz_ndr_nbt_TYPE_STRUCT: Heap-buffer-overflow in ndr_push_array_uint8 ClusterFuzz Unreproducible
38575	Bug	----	New	samba	2021-09-12	----	samba:fuzz_regfio: Timeout in fuzz_regfio ClusterFuzz Reproducible
38810	Bug	----	New	samba	2021-09-16	----	samba:fuzz_ndr_dnsserver_TYPE_STRUCT: Timeout in fuzz_ndr_dnsserver_TYPE_STRUCT ClusterFuzz Reproducible
48183	Bug	----	New	samba	2022-06-22	----	samba:fuzz_ndr_spoolss_TYPE_OUT: Null-dereference READ in ndr_push_spoolss_PrinterEnumValues ClusterFuzz Unreproducible
48234	Bug	----	New	samba	2022-06-23	----	samba:fuzz_ndr_dfsblobs_TYPE_STRUCT: Out-of-memory in fuzz_ndr_dfsblobs_TYPE_STRUCT ClusterFuzz Reproducible
48328	Bug	----	New	samba	2022-06-24	----	samba:fuzz_ldb_parse_tree: Timeout in fuzz_ldb_parse_tree ClusterFuzz Reproducible
48808	Bug	----	New	samba	2022-07-06	----	samba:fuzz_ndr_bkupblobs_TYPE_STRUCT: Timeout in fuzz_ndr_bkupblobs_TYPE_STRUCT ClusterFuzz Reproducible
50597	Bug	----	New	samba	2022-08-24	----	samba:fuzz_ndr_ioxidresolver: Timeout in fuzz_ndr_ioxidresolver ClusterFuzz Reproducible
50927	Bug	----	New	samba	2022-09-02	----	samba:fuzz_ndr_preg_TYPE_STRUCT: Timeout in fuzz_ndr_preg_TYPE_STRUCT ClusterFuzz Reproducible
53748	Bug	----	New	samba	2022-11-25	----	samba:fuzz_ndr_drsblobs_TYPE_STRUCT: Timeout in fuzz_ndr_drsblobs_TYPE_STRUCT ClusterFuzz Reproducible
53838	Bug	----	New	samba	2022-11-28	----	samba:fuzz_parse_lpq_entry: Integer-overflow in parse_lpq_entry ClusterFuzz Reproducible

1/13 unfixed bug in NBT

OSS-Fuzz false positives and excuses

realloc()-heavy code is 1000× slower when fuzzing with sanitisers

OSS-Fuzz memory (including stack) is very constrained

we fuzz some unused code

nobody looks much

OSS-Fuzz successes

CVE-2020-10704 — LDAP stack exhaustion
https://bugzilla.samba.org/show_bug.cgi?id=14334

39 patches saying “Credit to OSS-Fuzz”,
but I know we missed some.

several real bugs

often finds code that need general improvement

OSS-Fuzz problems

all the emails look the same

you need to login to Google

the bug-tracker is not great and not ours

90-day window can discourage fuzzing (I have fuzz targets in waiting)

example of OSS-Fuzz helping

last month we added transparent compression to NDR

it looked OK, seemed to work
and caused all manner of chaos in OSS-Fuzz

fixed within a week, affecting no releases

this *would* have lain round for years

Fuzzing outside of OSS-Fuzz

local fuzzing with Honggfuzz

triage and fix problems at your own pace

you *appear to* get it right the first time

Fuzzing outside of OSS-Fuzz

local fuzzing with Honggfuzz

triage and fix problems at your own pace

you *appear to* get it right the first time

2023 resolution: **no new features without fuzzers**

An example: LZXpress Huffman

yet another LZ77/Huffman compression algorithm

inherently gnarly code

last weeks of development were a fuzz/fix cycle

An example: LZXpress Huffman

yet another LZ77/Huffman compression algorithm

inherently gnarly code

last weeks of development were a fuzz/fix cycle

address sanitizer only; OSS-Fuzz still found things with UBSan

An example: LZXpress Huffman

yet another LZ77/Huffman compression algorithm

inherently gnarly code

last weeks of development were a fuzz/fix cycle

address sanitizer only; OSS-Fuzz still found things with UBSan

I can sleep at night

LZXpress Huffman fuzzers

decompression

compression

compress→decompress→compare round-trip

LZXpress Huffman fuzzers

decompression

compression

compress→decompress→compare round-trip

not the other round-trip (decompress→compress→compare)
there are many valid compressed forms

Example 2: SDDL parse fuzzer

preparatory work for conditional ACEs

SDDL fuzzer

```
sd1 = sddl_decode(mem_ctx, sddl_string, &dom_sid);
if (sd1 == NULL) {
        goto end;
}
result = sddl_encode(mem_ctx, sd1, &dom_sid);
sd2 = sddl_decode(mem_ctx, result, &dom_sid);
ok = security_descriptor_equal(sd1, sd2);
if (!ok) {
        abort();
}
```

SDDL fuzzer

```
sd1 = sddl_decode(mem_ctx, sddl_string, &dom_sid);
if (sd1 == NULL) {
        goto end;
}
result = sddl_encode(mem_ctx, sd1, &dom_sid);
sd2 = sddl_decode(mem_ctx, result, &dom_sid);
ok = security_descriptor_equal(sd1, sd2);
if (!ok) {
        abort();
}
```

expect bad strings, no worries

SDDL fuzzer

```
sd1 = sddl_decode(mem_ctx, sddl_string, &dom_sid);
if (sd1 == NULL) {
        goto end;
}
result = sddl_encode(mem_ctx, sd1, &dom_sid);
sd2 = sddl_decode(mem_ctx, result, &dom_sid);
ok = security_descriptor_equal(sd1, sd2);
if (!ok) {
        abort();
}
```

SDDL fuzzer

```
sd1 = sddl_decode(mem_ctx, sddl_string, &dom_sid);
if (sd1 == NULL) {
        goto end;
}
result = sddl_encode(mem_ctx, sd1, &dom_sid);
sd2 = sddl_decode(mem_ctx, result, &dom_sid);
ok = security_descriptor_equal(sd1, sd2);
if (!ok) {
        abort();
}
```

assert the security descriptors are the same

Ignoring non-uppercase letters in flags:

```
[make flags into its own little '\0'-terminated string]

while (str[0] != '\0' && isupper(str[0])) {
      if (str isn't a valid flag) {
          return false;
      }
}
return true;
```

Ignoring non-uppercase letters in flags:

```
00000000  44 3a 50 50 50 50 50 50  50 50 50 50 50 50 50 50  |D:PPPPPPPPPPPPPP|
00000010  50 50 50 50 50 50 50 50  50 50 50 50 50 50 50 50  |PPPPPPPPPPPPPPPP|
00000020  50 50 50 50 50 50 50 50  50 50 50 50 50 50 50 28  |PPPPPPPPPPPPPPP(|
00000030  76 54 41 41 72 34 37 41  41 41 41 da 41 41 41 41  |vTAAr47AAAA.AAAA|
00000040  41 41 3b 34 e7 8d f9 26  44 d7 b3 32 43 fd 45 76  |AA;4...&D..2C.Ev|
00000050  54 3b 3b 3b 0c 0c 28 ff  7e 28 b3 28 28 28 28 28  |T;;;..(.~(.(((((|
00000060  fd 45 76 54 3b 4d 31 e4  36 d2 32 43 fd 45 4f 41  |.EvT;M1.6.2C.EOA|
00000070  3a 34 e7 f9 26 bb d7 46  41 28 93 47 58 c3 72 f7  |:4..&..FA(.GX.r.|
00000080  ab 34 73 a5 32 31 e4 36  d2 93 c3 38 4c 4f ae ae  |.4s.21.6...8LO..|
00000090  ae ae ae ae ae ae ae 36  36 37 34 34 38 72 f7 ab  |.......667448r..|
```

Fuzz seeds looking more respectable...

```
00000000  44 3a 41 52 50 50 50 50  50 28 4f 4c 3b 3b 46 57  |D:ARPPPPP(OL;;FW|
00000010  3b 30 7e ff ff ff ff ff  ff ff 2d 31 38 f5 ff ff  |;0~.......-18...|
00000020  fb 3b 3b 52 43 29 28 4f  44 3b 3b 46 57 3b 3b 3b  |.;;RC)(OD;;FW;;;|
00000030  52 43 29 28 4f 44 3b 3b  46 57 3b 30 30 ff ff ff  |RC)(OD;;FW;00...|
00000040  fb 30 e9 9b 3c cf e6 f5  ff ff fb 3b 3b 52 43 29  |.0..<......;;RC)|
00000050  28 4f 44 3b 3b 46 57 43  52 3b 3b 3b 52 43 29 28  |(OD;;FWCR;;;RC)(|
00000060  4f 44 3b 3b 46 58 47 52  3b 3b 33 43 43 35 38 37  |OD;;FXGR;;3CC587|
00000070  32 35 44 44 44 44 44 44  44 44 44 44 44 44 44 44  |25DDDDDDDDDDDDDD|
00000080  44 44 44 44 44 44 44 44  44 44 3b 52 43 29 28 4f  |DDDDDDDDDD;RC)(O|
00000090  44 3b 3b 46 58 3b 3b 3b  52 43 29 28 4f 44 3b 3b  |D;;FX;;;RC)(OD;;|
```

Fuzz seeds looking more respectable...
but for the GUIDs

```
00000000  44 3a 41 52 50 50 50 50  50 28 4f 4c 3b 3b 46 57  |D:ARPPPPP(OL;;FW|
00000010  3b 30 7e ff ff ff ff ff  ff ff 2d 31 38 f5 ff ff  |;0~.......-18...|
00000020  fb 3b 3b 52 43 29 28 4f  44 3b 3b 46 57 3b 3b 3b  |.;;RC)(OD;;FW;;;|
00000030  52 43 29 28 4f 44 3b 3b  46 57 3b 30 30 ff ff ff  |RC)(OD;;FW;00...|
00000040  fb 30 e9 9b 3c cf e6 f5  ff ff fb 3b 3b 52 43 29  |.0..<......;;RC)|
00000050  28 4f 44 3b 3b 46 57 43  52 3b 3b 3b 52 43 29 28  |(OD;;FWCR;;;RC)(|
00000060  4f 44 3b 3b 46 58 47 52  3b 3b 33 43 43 35 38 37  |OD;;FXGR;;3CC587|
00000070  32 35 44 44 44 44 44 44  44 44 44 44 44 44 44 44  |25DDDDDDDDDDDDDD|
00000080  44 44 44 44 44 44 44 44  44 44 3b 52 43 29 28 4f  |DDDDDDDDDD;RC)(O|
00000090  44 3b 3b 46 58 3b 3b 3b  52 43 29 28 4f 44 3b 3b  |D;;FX;;;RC)(OD;;|
```

Non-standard GUIDs were always there:

```
00000000  44 3a 50 50 50 50 50 50  50 50 50 50 50 50 50 50  |D:PPPPPPPPPPPPPP|
00000010  50 50 50 50 50 50 50 50  50 50 50 50 50 50 50 50  |PPPPPPPPPPPPPPPP|
00000020  50 50 50 50 50 50 50 50  50 50 50 50 50 50 50 28  |PPPPPPPPPPPPPPP(|
00000030  76 54 41 41 72 34 37 41  41 41 41 da 41 41 41 41  |vTAAr47AAAA.AAAA|
00000040  41 41 3b 34 e7 8d f9 26  44 d7 b3 32 43 fd 45 76  |AA;4...&D..2C.Ev|
00000050  54 3b 3b 3b 0c 0c 28 ff  7e 28 b3 28 28 28 28 28  |T;;;..(.~(.(((((|
00000060  fd 45 76 54 3b 4d 31 e4  36 d2 32 43 fd 45 4f 41  |.EvT;M1.6.2C.EOA|
00000070  3a 34 e7 f9 26 bb d7 46  41 28 93 47 58 c3 72 f7  |:4..&..FA(.GX.r.|
00000080  ab 34 73 a5 32 31 e4 36  d2 93 c3 38 4c 4f ae ae  |.4s.21.6...8LO..|
00000090  ae ae ae ae ae ae ae 36  36 37 34 34 38 72 f7 ab  |.......667448r..|
```

Now the fuzzer seeds look more like this:

```
00000000  4f 3a 53 2d 31 2d 35 2d  38 34 2d 30 2d 30 2d 30  |O:S-1-5-84-0-0-0|
00000010  2d 30 2d 30 2d 30 30 30  32 2d 31 47 3a 53 2d 32  |-0-0-0002-1G:S-2|
00000020  35 2d 30 32 2d 31 2d 35  32 2d 30 30 32 2d 31 2d  |5-02-1-52-002-1-|
00000030  35 32 2d 30 30 30 32 2d  31 2d 30 32 2d 31 2d 35  |52-0002-1-02-1-5|
00000040  32 2d 30 30 30 32 53 3a  50 50 50 50 50 28 4f 4c  |2-0002S:PPPPP(OL|
00000050  3b 3b 53 44 46 41 47 52  3b 43 41 32 33 37 41 43  |;;SDFAGR;CA237AC|
00000060  41 2d 41 41 41 41 2d 45  39 44 63 2d 42 41 30 32  |A-AAAA-E9Dc-BA02|
00000070  2d 44 64 46 32 32 32 31  37 37 39 45 38 3b 34 36  |-DdF2221779E8;46|
00000080  38 32 34 66 39 41 2d 44  36 43 41 2d 31 33 38 63  |824f9A-D6CA-138c|
00000090  2d 45 39 30 32 2d 31 34  31 41 35 36 35 39 30 35  |-E902-141A565905|
000000a0  34 38 3b 52 43 29 28 4f  4c 3b 3b 53 44 47 52 3b  |48;RC)(OL;;SDGR;|
```

Fuzzing is going OK

the OSS-Fuzz user experience could be improved

it could be better integrated into Samba workflows

fuzzing makes Samba better

any questions?