

ProveNFix: Temporal Property guided Program Repair

(Appendix)

YAHUI SONG, National University of Singapore, Singapore

XIANG GAO, Beihang University, China

WENHUA LI, National University of Singapore, Singapore

WEI-NGAN CHIN, National University of Singapore, Singapore

ABHIK ROYCHOUDHURY, National University of Singapore, Singapore

ACM Reference Format:

Yahui Song, Xiang Gao, Wenhua Li, Wei-Ngan Chin, and Abhik Roychoudhury. 2024. ProveNFix: Temporal Property guided Program Repair: (Appendix). *Proc. ACM Softw. Eng.* 1, FSE, Article 11 (July 2024), 16 pages. <https://doi.org/10.1145/3643737>

This file is the supplementary material for the submission #142 of FSE 2024. The source code and evaluation benchmarks are openly accessible from [3].

A TRANSLATION FROM LTL FORMULAE TO REGULAR EXPRESSIONS

As a variation of the regular expression, *IntRE* naturally encodes linear temporal logic (LTL) formulae with arithmetic constraints for the case analysis. Although the underlying reasoning is based on the form presented in Fig.10, we support LTL formulae by syntax, and recursively convert them into temporal constraints in *IntRE*.

Classical LTL extended propositional logic with the temporal operators \mathcal{G} (“globally”) and \mathcal{F} (“finally”). Subsequently, LTL was extended to include the \mathcal{X} (“next time”) operator¹, \mathcal{U} (“until”) operator² and \mathcal{R} (“release”) operator³. As shown in Table 1, we encode these basic operators

Table 1. Selected translation examples for converting LTL formulae into *IntRE*. (I, J are events, and $_$ matches to all the events)

Post/future-conditions	
$\mathcal{G} I \equiv I^*$	$\mathcal{F} I \equiv _ * \cdot I$
$I \mathcal{U} J \equiv I^* \cdot J$	$I \rightarrow \mathcal{F} J \equiv \neg I \vee _ * \cdot J$
$\mathcal{X} I \equiv _ \cdot I$	$\mathcal{G} \mathcal{F} I \equiv (_ * \cdot I)^*$
$\mathcal{F} \mathcal{G} I \equiv _ * \cdot I^*$	$I \mathcal{R} J \equiv (J^* \cdot (I \wedge J)) \vee J^*$
Pre-conditions (past-time LTL)	
$\overleftarrow{\mathcal{G}} I \equiv I^*$	$\overleftarrow{\mathcal{F}} I \equiv I \cdot _ *$
$I \mathcal{S} J \equiv J \cdot I^*$	$\mathcal{P} I \equiv _ * \cdot I$

¹ $\mathcal{X} I$ means that I has to hold at the next state.

² $I \mathcal{U} J$ means that I has to hold at least until J becomes true.

³ $I \mathcal{R} J$ means that J has to be true until and including the point where I first becomes true; if I never becomes true, J must remain true forever.

Authors' addresses: [Yahui Song](#), National University of Singapore, , Singapore, yahui_s@nus.edu.sg; [Xiang Gao](#), Beihang University, , China, xiang_gao@buaa.edu.cn; [Wenhua Li](#), National University of Singapore, , Singapore, liwenhua@comp.nus.edu.sg; [Wei-Ngan Chin](#), National University of Singapore, , Singapore, chinwn@comp.nus.edu.sg; [Abhik Roychoudhury](#), National University of Singapore, , Singapore, abhik@comp.nus.edu.sg.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

© 2024 Copyright held by the owner/author(s).

ACM 2994-970X/2024/7-ART11

<https://doi.org/10.1145/3643737>

into our logic, making it more intuitive and readable, mainly when nested operators occur. Furthermore, by putting *IntRE* formulae in the precondition, our approach naturally composites *past-time LTL* [1, 2], which has the operators: $\overleftarrow{\mathcal{G}}$ (a reversed versions of \mathcal{G}); $\overleftarrow{\mathcal{F}}$ (a reversed versions of \mathcal{F}); \mathcal{P} for “previous” (a reversed versions of \mathcal{X}); and \mathcal{S} for “since” (a reversed versions of \mathcal{U}).

B SPECIFICATIONS FOR 17 PRIMITIVE APIS

```

1  int open(const char *path, int oflag, ... ); // For Resource Leak
2  // future: ret>0  $\wedge$   $\mathcal{F}$  (close(ret))
3
4  int socket(int domain, int type, int protocol); // For Resource Leak
5  // future: ret>0  $\wedge$   $\mathcal{F}$  (close(ret))
6
7  FILE *fopen(const char *file_name, const char *mode_of_operation);
8  // future: ret $\neq$ null  $\wedge$   $\mathcal{G}$  (!_(ret))  $\vee$  ret $\neq$ null  $\wedge$   $\mathcal{F}$  (fclose(ret)) // For Resource Leak
9
10 FILE *fdopen(int fd, const char *mode); // For Resource Leak
11 // future: ret $\neq$ null  $\wedge$   $\mathcal{G}$  (!_(ret))  $\vee$  ret $\neq$ null  $\wedge$   $\mathcal{F}$  (fclose(ret))
12
13 DIR *opendir(const char *name); // For Resource Leak
14 // future: ret>0  $\wedge$   $\mathcal{F}$  (closedir(ret))
15
16 int close(int fildes); // For Resource Leak
17 // post: (true  $\wedge$  close(fildes))
18
19 int fclose(FILE *stream); // For Resource Leak
20 // post: (true  $\wedge$  fclose(stream))
21
22 int endmntent(FILE *stream); // For Resource Leak
23 // post: (true  $\wedge$  fclose(stream))
24
25 int fflush(FILE *stream); // For Resource Leak
26 // post: (true  $\wedge$  fclose(stream))
27
28 int closedir(DIR *dirp); // For Resource Leak
29 // post: (true  $\wedge$  closedir(dirp))
30
31 void *malloc(size_t size); // For Null Pointer Dereference
32 // future: ret=null  $\wedge$   $\mathcal{G}$  (!deref(ret))
33
34 void *realloc(void *ptr, size_t size); // For Null Pointer Dereference
35 // future: ret=null  $\wedge$   $\mathcal{G}$  (!deref(ret))
36
37 void *calloc(size_t nitems, size_t size); // For Null Pointer Dereference
38 // future: ret=null  $\wedge$   $\mathcal{G}$  (!deref(ret))
39
40 struct tm *localtime(const time_t *timer); // For Null Pointer Dereference
41 // future: ret=null  $\wedge$   $\mathcal{G}$  (!deref(ret))
42
43 void -> (void *ptr, char *filed); // For Null Pointer Dereference
44 // post: (true  $\wedge$  deref(ptr)) // Pointer Dereference
45
46 void free (void *ptr); // For Memory Usage
47 // pre: true  $\wedge$   $\overleftarrow{\mathcal{F}}$  (malloc(ptr))
48 // post: (ptr=null  $\wedge$   $\epsilon$ )  $\vee$  (ptr $\neq$ null  $\wedge$  free(ptr))
49 // future: ptr $\neq$ null  $\wedge$   $\mathcal{G}$  (!_(ptr))
50
51 void *malloc (size_t size); // For Memory Usage
52 // pre: size>0  $\wedge$   $\_*$ 
53 // post: (ret=null  $\wedge$   $\epsilon$ )  $\vee$  (ret $\neq$ null  $\wedge$  malloc(ret))
54 // future: ret $\neq$ null  $\wedge$   $\mathcal{F}$  (free(ret))

```

C ALL THE BUGS FOUND IN TABLE 2 BY PROVENFIX

This section records all the bugs reported by PROVENFIX, and each record follows the following format:

Fix status, Project, Bug type, File, Function name, Failed API @ line number, Fix location.

In particular, there are two kinds of fix status: (Fixed) and (Found but not Fixed).

C.1 Swoole project

```

1 (Fixed), Swoole, Null Dereference, swoole_event.c, zif_swoole_event_set, swReactor_get @454, 455
2 (Fixed), Swoole, Null Dereference, swoole_event.c, zif_swoole_event_del, swReactor_get @553, 560
3 (Fixed), Swoole, Null Dereference, src/reactor/ReactorBase.c, swReactor_add, swReactor_get @147, 151
4 (Fixed), Swoole, Null Dereference, src/reactor/ReactorBase.c, swReactor_del, swReactor_get @160, 162
5 (Fixed), Swoole, Null Dereference, src/reactor/ReactorBase.c, swReactor_set, swReactor_get @168, 169
6 (Fixed), Swoole, Null Dereference, src/reactor/ReactorBase.c, swReactor_close, swReactor_get @253, 260
7 (Fixed), Swoole, Null Dereference, src/reactor/ReactorBase.c, swReactor_write, swReactor_get @274, 287,
  366
8 (Fixed), Swoole, Null Dereference, src/reactor/ReactorBase.c, swReactor_onWrite, swReactor_get @393, 422
9 (Fixed), Swoole, Null Dereference, src/network/Worker.c, swWorker_signal_handler, swReactor_get @98, 99
10 (Fixed), Swoole, Null Dereference, src/core/log.c, swLog_put, localtime @73, 74
11 (Fixed), Swoole, Null Dereference, swoole_mysql.c, zim_swoole_mysql_close, swReactor_get @1009, 1010
12 (Fixed), Swoole, Null Dereference, swoole_server.c, PHP_METHOD(swoole_server, __construct), malloc @1271,
  1294
13 (Fixed), Swoole, Null Dereference, src/memory/Table.c, swTableColumn_add, malloc @85, 128, 87
14 (Fixed), Swoole, Null Dereference, src/reactor/ReactorSelect.c, swReactorSelect_add, malloc @96, 99
15 (Fixed), Swoole, Null Dereference, swoole_client.c, client_onReceive, swoole_get_property @296, 297
16 (Fixed), Swoole, Null Dereference, swoole_http_client.c, http_client_onMessage, swoole_get_property @594,
  595
17 (Fixed), Swoole, Null Dereference, swoole_http_client.c, http_client_onReceive, swoole_get_property @660,
  661
18 (Fixed), Swoole, Null Dereference, swoole_http_client.c, http_client_send_http_request,
  swoole_get_property @803, 1053
19 (Fixed), Swoole, Null Dereference, swoole_http_client.c, zim_swoole_http_client_setMethod,
  swoole_get_property @1409, 1410
20 (Fixed), Swoole, Null Dereference, swoole_http_client.c, zim_swoole_http_client_upgrade,
  swoole_get_property @1831, 1832
21 (Fixed), Swoole, Null Dereference, swoole_client.c, client_execute_callback, swoole_get_property @101,
  107
22 (Fixed), Swoole, Null Dereference, src/network/Server.c, swServer_confirm, swServer_connection_verify
  @878, 879
23 (Fixed), Swoole, Null Dereference, src/network/ReactorThread.c, swReactorThread_onWrite,
  swServer_connection_get @870, 871
24 (Fixed), Swoole, Null Dereference, src/network/ReactorThread.c, swReactorThread_onPipeReceive,
  swServer_get_worker @436, 438
25 (Fixed), Swoole, Null Dereference, src/network/Worker.c, swWorker_onStop, swServer_get_worker @416, 420
26 (Fixed), Swoole, Null Dereference, src/network/Worker.c, swWorker_loop, swReactor_get @505, 506
27 (Fixed), Swoole, Null Dereference, src/reactor/ReactorBase.c, swReactor_wait_write_buffer, swReactor_get
  @454, 457
28 (Fixed), Swoole, Null Dereference, src/network/Port.c, swPort_onRead_http, malloc @310, 319
29 (Fixed), Swoole, Null Dereference, include/Server.h, swWorker_get_send_pipe, swServer_get_worker @892,
  893
30 (Fixed), Swoole, Null Dereference, src/core/socket.c, swSocket_wait_multi, calloc @122, 138
31 (Fixed), Swoole, Null Dereference, src/reactor/ReactorQueue.c, swReactorQueue_del, swReactor_get @223,
  236
32 (Fixed), Swoole, Null Dereference, swoole_http_client.c, zim_swoole_http_client_on, swoole_get_property
  @1477, 1482
33 (Fixed), Swoole, Null Dereference, swoole_http_client.c, PHP_METHOD(swoole_http_client, post),
  swoole_get_property @1811, 1814
34 (Fixed), Swoole, Null Dereference, swoole_http_client.c, PHP_METHOD(swoole_http_client, download),
  swoole_get_property @1783, 1787
35 (Fixed), Swoole, Null Dereference, swoole_http_client.c, PHP_METHOD(swoole_http_client, addFile),
  swoole_get_property @1372, 1382
36 (Fixed), Swoole, Null Dereference, swoole_http_client.c, PHP_METHOD(swoole_http_client, setData),
  swoole_get_property @1312, 1314
37 (Fixed), Swoole, Null Dereference, swoole_http_client.c, PHP_METHOD(swoole_http_client, setCookies),
  swoole_get_property @1297, 1299
38 (Fixed), Swoole, Null Dereference, swoole_http_client.c, PHP_METHOD(swoole_http_client, setHeaders),
  swoole_get_property @1283, 1285

```

```

39 (Fixed), Swoole, Null Dereference, swoole_http_client.c, http_client_execute, swoole_get_property @372,
    374
40 (Fixed), Swoole, Null Dereference, swoole_event.c, zif_swoole_event_add, swReactor_get @380, 382
41 (Fixed), Swoole, Null Dereference, swoole_mysql.c, zim_swoole_mysql_connect, swReactor_get @894, 896
42 (Fixed), Swoole, Null Dereference, swoole_mysql.c, swoole_mysql_onRead, swReactor_get @1386, 1387
43 (Fixed), Swoole, Null Dereference, src/network/Worker.c, swWorker_loop, swServer_get_worker @469, 487
44 (Fixed), Swoole, Null Dereference, src/factory/FactoryProcess.c, swFactoryProcess_finish,
    swServer_get_worker @213, 220
45 (Fixed), Swoole, Null Dereference, src/reactor/ReactorSelect.c, swReactorSelect_wait, swReactor_get @236,
    259
46 (Fixed), Swoole, Null Dereference, src/reactor/ReactorPoll.c, swReactorPoll_wait, swReactor_get @243, 267
47 (Fixed), Swoole, Null Dereference, src/reactor/ReactorQueue.c, swReactorQueue_wait, swReactor_get @323,
    326
48 (Fixed), Swoole, Null Dereference, src/network/ReactorProcess.c, swReactorProcess_loop, swReactor_get
    @352, 353
49 (Fixed), Swoole, Null Dereference, src/network/Manager.c, swManager_start, calloc @94, 103
50 (Fixed), Swoole, Null Dereference, src/network/Worker.c, swWorker_onStart, swServer_get_worker @393, 399
51 (Fixed), Swoole, Null Dereference, src/network/Worker.c, swWorker_clean, swServer_get_worker @432, 435
52 (Fixed), Swoole, Null Dereference, src/network/Worker.c, swWorker_loop, swReactor_get @503, 504
53 (Fixed), Swoole, Null Dereference, src/protocol/Redis.c, swRedis_recv, malloc @47, 111
54 (Fixed), Swoole, Memory Leak, src/core/hashmap.c, swHashMap_new, malloc @95, 118
55 (Fixed), Swoole, Memory Leak, src/core/hashmap.c, swHashMap_new, malloc @114, 130
56 (Fixed), Swoole, Memory Leak, src/memory/Table.c, swTableColumn_add, malloc @85, 85
57 (Fixed), Swoole, Memory Leak, src/memory/Table.c, swTableColumn_add, malloc @85, 131
58 (Fixed), Swoole, Memory Leak, src/memory/Table.c, swTable_new, malloc @63, 72, 80
59 (Fixed), Swoole, Memory Leak, src/reactor/ReactorPoll.c, swReactorPoll_create, malloc @42, 54
60 (Fixed), Swoole, Memory Leak, src/reactor/ReactorPoll.c, swReactorPoll_create, malloc @42, 60
61 (Fixed), Swoole, Memory Leak, src/pipe/PipeBase.c, swPipeBase_create, malloc @32, 42
62 (Fixed), Swoole, Memory Leak, src/pipe/PipeEventfd.c, swPipeEventfd_create, malloc @35, 68
63 (Fixed), Swoole, Memory Leak, src/pipe/PipeUnsock.c, swPipeUnsock_create, malloc @54, 65
64 (Fixed), Swoole, Memory Leak, src/network/Server.c, swServer_create_worker_buffer, malloc @464, 476
65 (Fixed), Swoole, Memory Leak, src/network/Timer.c, swTimer_add, malloc @115, 125
66 (Fixed), Swoole, Memory Leak, swoole_server.c, PHP_METHOD(swoole_server, __construct), malloc @1271, 1321,
67 (Fixed), Swoole, Memory Leak, swoole_server.c, PHP_METHOD(swoole_server, __construct), malloc @1271, 1303
68 (Fixed), Swoole, Memory Leak, swoole_server.c, PHP_METHOD(swoole_server, __construct), malloc @1271, 1277
69 (Fixed), Swoole, Memory Leak, src/core/base.c, swoole_gethostbyname, malloc @916, 958
70 (Fixed), Swoole, Memory Leak, src/core/hashmap.c, swHashMap_new, malloc @126, 137
71 (Fixed), Swoole, Memory Leak, src/factory/FactoryThread.c, swFactoryThread_dispatch, malloc @164, 177
72 (Fixed), Swoole, Memory Leak, src/factory/FactoryThread.c, swFactoryThread_dispatch, malloc @164, 181
73 (Fixed), Swoole, Memory Leak, src/os/base.c, swAioBase_write, malloc @304, 325,
74 (Fixed), Swoole, Memory Leak, src/os/base.c, swAioBase_write, malloc @304, 322
75 (Fixed), Swoole, Memory Leak, src/os/base.c, swAio_dns_lookup, malloc @331, 347
76 (Fixed), Swoole, Memory Leak, src/os/base.c, swAio_dns_lookup, malloc @331, 352
77 (Fixed), Swoole, Memory Leak, src/os/base.c, swAioBase_read, malloc @358, 375
78 (Fixed), Swoole, Memory Leak, src/os/base.c, swAioBase_read, malloc @358, 380
79 (Fixed), Swoole, Memory Leak, src/core/hashmap.c, swHashMap_new, malloc @95, 130
80 (Fixed), Swoole, Memory Leak, src/core/hashmap.c, swHashMap_new, malloc @114, 137
81 (Fixed), Swoole, Memory Leak, src/network/ReactorThread.c, swReactorThread_loop, malloc @1218
82 (fixed), Swoole, Resource Leak, src/core/socket.c, swSocket_sendfile_async, open @25, 36 , *
83 (fixed), Swoole, Resource Leak, src/core/base.c, swoole_file_get_contents, open @554, 563 , *
84 (fixed), Swoole, Resource Leak, src/network/ReactorProcess.c, swReactorProcess_reuse_port,
    swSocket_create @541, 551
85 (fixed), Swoole, Resource Leak, swoole_async.c, PHP_FUNCTION(swoole_async_read), open @348, 358
86 (fixed), Swoole, Resource Leak, swoole_async.c, PHP_FUNCTION(swoole_async_read), open @348, 363
87 (fixed), Swoole, Resource Leak, swoole_async.c, PHP_FUNCTION(swoole_async_read), open @348, 370
88 (fixed), Swoole, Resource Leak, swoole_async.c, PHP_FUNCTION(swoole_async_readfile), open @528, 537
89 (fixed), Swoole, Resource Leak, swoole_async.c, PHP_FUNCTION(swoole_async_readfile), open @528, 542
90 (fixed), Swoole, Resource Leak, swoole_async.c, PHP_FUNCTION(swoole_async_readfile), open @528, 547
91 (fixed), Swoole, Resource Leak, swoole_mmap.c, PHP_METHOD(swoole_mmap, open), open @172, 184
92 (fixed), Swoole, Resource Leak, swoole_mmap.c, PHP_METHOD(swoole_mmap, open), open @172, 189
93 (fixed), Swoole, Resource Leak, swoole_mmap.c, PHP_METHOD(swoole_mmap, open), open @172, 205
94 (fixed), Swoole, Resource Leak, swoole_lock.c, PHP_METHOD(swoole_lock, __construct), open @99, 123
95 (fixed), Swoole, Resource Leak, swoole_http_client.c, http_client_execute, open @381, 400
96 (fixed), Swoole, Resource Leak, src/network/Server.c, swServer_add_port, swSocket_create @1131, 1140
97 (fixed), Swoole, Resource Leak, src/network/Client.c, swClient_create, socket @84, 106
98 (fixed), Swoole, Resource Leak, src/core/base.c, swoole_system_random, open @379, 392
99 (fixed), Swoole, Resource Leak, src/core/base.c, swoole_system_random, open @379, 394
100 (fixed), Swoole, Resource Leak, swoole_lock.c, PHP_METHOD(swoole_lock, __construct), open @99, 126

```

C.2 lxc project

```

1 (Fixed), Lxc, Null Dereference, src/lxc/tools/lxc_autostart.c, get_list, malloc @231, 232
2 (Fixed), Lxc, Null Dereference, src/lxc/initutils.c, lxc_global_config_value, malloc @126, 129
3 (Fixed), Lxc, Null Dereference, src/lxc/initutils.c, lxc_global_config_value, malloc @126, 130
4 (Fixed), Lxc, Null Dereference, src/lxc/initutils.c, lxc_global_config_value, malloc @126, 131
5 (Fixed), Lxc, Null Dereference, src/lxc/lxccontainer.c, do_bdev_create, lxcapi_get_config_path @1060,
  1061
6 (Fixed), Lxc, Null Dereference, src/lxc/cgroups/cgfs.c, subsystems_from_mount_options, malloc @1804, 1805
7 (Fixed), Lxc, Null Dereference, src/lxc/initutils.c, lxc_global_config_value, malloc @127, 130
8 (Fixed), Lxc, Null Dereference, src/lxc/initutils.c, lxc_global_config_value, malloc @125, 129
9 (Fixed), Lxc, Null Dereference, src/lxc/conf.c, append_ptyname, malloc @862, 863
10 (Fixed), Lxc, Null Dereference, src/lxc/confile.c, set_config_environment, malloc @1531, 1545
11 (Fixed), Lxc, Null Dereference, src/lxc/confile.c, set_config_cgroup, malloc @1822, 1844
12 (Fixed), Lxc, Null Dereference, src/lxc/confile.c, set_config_limit, malloc @1938, 1959
13 (Fixed), Lxc, Null Dereference, src/lxc/confile.c, set_config_idmaps, malloc @1983, 2010
14 (Fixed), Lxc, Null Dereference, src/lxc/confile.c, set_config_idmaps, malloc @1979, 2010
15 (Fixed), Lxc, Null Dereference, src/lxc/attach.c, lsm_set_label_at, malloc @146, 176
16 (Fixed), Lxc, Null Dereference, src/lxc/network.c, is_wlan, malloc @163, 165
17 (Fixed), Lxc, Null Dereference, src/lxc/tools/lxc_copy.c, set_mnt_entry, malloc @336, 376
18 (Fixed), Lxc, Null Dereference, src/lxc/tools/lxc_copy.c, set_mnt_entry, malloc @349, 376
19 (Fixed), Lxc, Null Dereference, src/lxc/tools/lxc_copy.c, set_mnt_entry, malloc @362, 376
20 (Fixed), Lxc, Null Dereference, src/lxc/tools/lxc_copy.c, mount_tmpfs, malloc @850, 898
21 (Fixed), Lxc, Null Dereference, src/lxc/tools/lxc_info.c, print_info, malloc @368, 378
22 (Fixed), Lxc, Null Dereference, src/lxc/tools/lxc_ls.c, ls_get_groups, malloc @617, 619
23 (Fixed), Lxc, Null Dereference, src/lxc/tools/lxc_ls.c, ls_recv_str, malloc @1116, 1117
24 (Fixed), Lxc, Null Dereference, src/lxc/tools/lxc_monitor.c, main, malloc @155, 209
25 (Fixed), Lxc, Memory Leak, src/lxc/bdev/lxcrsync.c, do_rsync, malloc @57, 65
26 (Fixed), Lxc, Memory Leak, src/lxc/commands.c, lxc_cmd_rsp_recv, malloc @216, 230, 224
27 (Fixed), Lxc, Memory Leak, src/lxc/confile_network_legacy.c, set_config_network_legacy_ipv4, malloc @562,
  611
28 (Fixed), Lxc, Memory Leak, src/lxc/confile_network_legacy.c, set_config_network_legacy_ipv6, malloc @692,
  694,
29 (Fixed), Lxc, Memory Leak, src/lxc/lxccontainer.c, do_lxcapi_migrate, malloc @4051, 4089
30 (Fixed), Lxc, Memory Leak, src/lxc/bdev/bdev.c, do_mkfs_exec_wrapper, malloc @752, 762
31 (Fixed), Lxc, Memory Leak, src/lxc/bdev/bdev.c, do_mkfs_exec_wrapper, malloc @752, 758
32 (Fixed), Lxc, Memory Leak, src/lxc/confile.c, set_config_net_ipv4, malloc @1018, 1069
33 (Fixed), Lxc, Memory Leak, src/lxc/confile.c, set_config_net_ipv6, malloc @1154, 1172
34 (Fixed), Lxc, Memory Leak, src/lxc/confile.c, set_config_net_nic, lxc_get_netdev_by_idx @4089, 4093
35 (Fixed), Lxc, Memory Leak, src/lxc/commands.c, lxc_cmd_state_server_callback, malloc @988, 1007
36 (Fixed), Lxc, Memory Leak, src/lxc/bdev/bdev.c, bdev_copy, malloc @339, 349
37 (Fixed), Lxc, Memory Leak, src/lxc/start.c, lxc_recv_ttys_from_child, malloc @1133, 1139
38 (Fixed), Lxc, Memory Leak, src/lxc/start.c, lxc_recv_ttys_from_child, malloc @1133, 1161
39 (Fixed), Lxc, Memory Leak, src/lxc/conf.c, lxc_create_tty, malloc @3672, 3689
40 (Fixed), Lxc, Memory Leak, src/lxc/conf.c, lxc_create_tty, malloc @3672, 3714
41 (Fixed), Lxc, Memory Leak, src/lxc/conf.c, clr_config_net_nic, lxc_get_netdev_by_idx @4134, 4138
42 (Fixed), Lxc, Memory Leak, src/lxc/conf.c, get_config_net_nic, lxc_get_netdev_by_idx @4429, 4433
43 (Fixed), Lxc, Memory Leak, src/lxc/lxcutmp.c, lxc_utmp_mainloop_add, malloc @344, 355
44 (Fixed), Lxc, Memory Leak, src/lxc/network.c, ifa_get_local_ip, malloc @1135, 1143
45 (Fixed), Lxc, Memory Leak, tools/lxc_autostart.c, get_list, malloc @231, 248
46 (Fixed), Lxc, Memory Leak, src/lxc/confile_network_legacy.c, set_config_network_legacy_ipv6, malloc @692,
  716
47 (Fixed), Lxc, Resource Leak, src/lxc/tools/lxc_usernsexec.c, opentty, open @83, 92
48 (Fixed), Lxc, Resource Leak, src/lxc/tools/lxc_usernsexec.c, opentty, open @83, 100
49 (Fixed), Lxc, Resource Leak, src/lxc/bdev/lxczfs.c, zfs_clone, open @174, 178
50 (Fixed), Lxc, Resource Leak, src/lxc/attach.c, lxc_proc_get_context_info, fopen @201, 210
51 (Fixed), Lxc, Resource Leak, src/lxc/monitor.c, lxc_monitor_open, socket @218, 231
52 (Fixed), Lxc, Resource Leak, src/lxc/bdev/bdev.c, detect_fs, fopen @710, 717
53 (Fixed), Lxc, Resource Leak, src/lxc/bdev/bdev.c, detect_fs, fopen @710, 723
54 (Fixed), Lxc, Resource Leak, src/lxc/bdev/bdev.c, detect_fs, fopen @710, 727
55 (Fixed), Lxc, Resource Leak, src/lxc/bdev/bdev.c, detect_fs, fopen @710, 731
56 (Fixed), Lxc, Resource Leak, src/lxc/bdev/bdev.c, detect_fs, fopen @710, 733

```

C.3 WavPack project

```

1 (Fixed), WavPack, Null Dereference, src/open_filename.c, WavpackOpenFileInput, malloc @253, 255
2 (Fixed), WavPack, Null Dereference, src/open_legacy, WavpackOpenFileInputEx, malloc @102, 104
3 (Fixed), WavPack, Null Dereference, src/open_legacy, WavpackOpenFileInputEx, malloc @108, 110
4 (Fixed), WavPack, Null Dereference, cli/import_id3.c, Latin1ToUTF8, malloc @447, 455
5 (Fixed), WavPack, Null Dereference, cli/wavpack.c, TextToUTF8, malloc @4123, 4141

```

```

6 (Fixed), WavPack, Null Dereference, cli/wvunpack.c, UTF8ToAnsi, malloc @2787, 2796
7 (Fixed), WavPack, Null Dereference, src/open_raw.c, WavpackOpenRawDecoder, malloc @150, 151
8 (Fixed), WavPack, Null Dereference, src/open_raw.c, WavpackOpenRawDecoder, malloc @283, 284
9 (Fixed), WavPack, Null Dereference, src/open_raw.c, WavpackOpenRawDecoder, malloc @154, 155
10 (Fixed), WavPack, Null Dereference, src/open_raw.c, WavpackOpenRawDecoder, malloc @202, 203
11 (Fixed), WavPack, Null Dereference, cli/wavpack.c, wild_fopen, malloc @1478, 1479
12 (Fixed), WavPack, Null Dereference, cli/wvtag.c, malloc @1080, 1288
13 (Fixed), WavPack, Null Dereference, cli/wvtag.c, wild_fopen, malloc @1640, 1641
14 (Fixed), WavPack, Null Dereference, cli/wvtag.c, TextToUTF8, malloc @1511, 1529
15 (Fixed), WavPack, Null Dereference, cli/wvtag.c, UTF8ToAnsi, malloc @1364, 1373
16 (Fixed), WavPack, Null Dereference, src/open_utils.c, read_channel_identities, malloc @506, 507
17 (Fixed), WavPack, Null Dereference, cli/wvunpack.c, open_output_file, malloc @944, 947
18 (Fixed), WavPack, Null Dereference, cli/wvunpack.c, unpack_dsd_audio, malloc @1690, 1693
19 (Fixed), WavPack, Null Dereference, src/unpack_dsd.c, init_dsd_block_fast, malloc @147, 174
20 (Fixed), WavPack, Null Dereference, src/unpack_dsd.c, init_dsd_block_fast, malloc @144, 145
21 (Fixed), WavPack, Null Dereference, cli/wvunpack.c, unpack_dsd_audio, malloc @1543, 1546
22 (Fixed), WavPack, Null Dereference, src/open_raw.c, WavpackOpenRawDecoder, malloc @249, 250
23 (Fixed), WavPack, Null Dereference, src/open_raw.c, WavpackOpenRawDecoder, malloc @296, 299
24 (Fixed), WavPack, Null Dereference, src/open_raw.c, WavpackOpenRawDecoder, malloc @293, 294
25 (Fixed), WavPack, Null Dereference, src/open_raw.c, WavpackOpenRawDecoder, malloc @286, 289
26 (Fixed), WavPack, Null Dereference, src/pack_dsd.c, encode_buffer_fast, malloc @324, 325
27 (Fixed), WavPack, Null Dereference, cli/wavpack.c, pack_audio, malloc @2276, 2337
28 (Fixed), WavPack, Null Dereference, cli/wavpack.c, repack_audio, malloc @3230, 3233
29 (Fixed), WavPack, Null Dereference, cli/wavpack.c, repack_audio, malloc @3241, 3266
30 (Fixed), WavPack, Null Dereference, cli/wavpack.c, verify_audio, malloc @3464, 3467
31 (Fixed), WavPack, Null Dereference, /cli/wvunpack.c, do_tag_extractions, malloc @1826, 1827
32 (Fixed), WavPack, Null Dereference, /cli/wvunpack.c, dump_tag_item_to_file, malloc @2557, 2561
33 (Fixed), WavPack, Null Dereference, src/open_raw.c, WavpackOpenRawDecoder, malloc @2132, 203
34 (Fixed), WavPack, Null Dereference, src/pack_utils.c, pack_streams, malloc @933, 965
35 (Fixed), WavPack, Null Dereference, cli/wavpack.c, unreorder_channels, malloc @3401, 3407
36 (Fixed), WavPack, Null Dereference, cli/wavpack.c, unreorder_channels, malloc @2132, 2138
37 (Fixed), WavPack, Null Dereference, cli/wvtag.c, do_tag_extractions, malloc @936, 937
38 (Fixed), WavPack, Null Dereference, cli/wvtag.c, clear_tag_items, malloc @1041, 1044
39 (Fixed), WavPack, Null Dereference, cli/wvtag.c, list_tags_to_file, malloc @1077, 1100
40 (Fixed), WavPack, Null Dereference, cli/wvtag.c, dump_tag_item_to_file, malloc @1196, 1200
41 (Fixed), WavPack, Null Dereference, cli/wvtag.c, calculate_tag_size, malloc @1264, 1268
42 (Fixed), WavPack, Memory Leak, cli/wavpack.c, reorder_channels, malloc @3375, 3392
43 (Fixed), WavPack, Memory Leak, cli/wavpack.c, TextToUTF8, malloc @4123, 4138
44 (Fixed), WavPack, Memory Leak, cli/wvtag.c, TextToUTF8, malloc @1511, 1526
45 (Fixed), WavPack, Memory Leak, src/open_utils.c, read_wvc_block, malloc @997, 1024
46 (Fixed), WavPack, Memory Leak, src/pack_utils.c, WavpackPackInit, malloc @540, 550
47 (Fixed), WavPack, Memory Leak, cli/wavpack.c, repack_audio, malloc @3230, 3280
48 (Fixed), WavPack, Memory Leak, cli/wavpack.c, repack_audio, malloc @3230, 3332
49 (Fixed), WavPack, Memory Leak, cli/wavpack.c, repack_audio, malloc @3223, 3365,
50 (Fixed), WavPack, Memory Leak, cli/wavpack.c, repack_audio, malloc @3223, 3357,
51 (Fixed), WavPack, Memory Leak, cli/wavpack.c, repack_audio, malloc @3223, 3332
52 (Fixed), WavPack, Memory Leak, cli/wavpack.c, unreorder_channels, malloc @3401, 3409
53 (Fixed), WavPack, Memory Leak, cli/wavpack.c, unreorder_channels, malloc @2132, 2140

```

C.4 flex project

```

1 (Fixed), Flex, Null Dereference, src/filter.c, filter_tee_header, fdopen @245, 247
2 (Fixed), Flex, Null Dereference, src/filter.c, filter_fix_linedirs, regmatch_dup @360, 362
3 (Fixed), Flex, Null Dereference, src/gen.c, mkeoltbl, calloc @114, 116
4 (Fixed), Flex, Null Dereference, src/gen.c, mkeoltbl, calloc @109, 111
5 (Fixed), Flex, Null Dereference, src/gen.c, mkcttbl, calloc @216, 218
6 (Fixed), Flex, Null Dereference, src/gen.c, mkssltbl, calloc @312, 314
7 (Fixed), Flex, Null Dereference, src/gen.c, mkssltbl, calloc @319, 321
8 (Fixed), Flex, Null Dereference, src/gen.c, mkecsttbl, calloc @442, 444
9 (Fixed), Flex, Null Dereference, src/gen.c, mkecsttbl, calloc @449, 451
10 (Fixed), Flex, Null Dereference, src/gen.c, mkfttbl, calloc @653, 655
11 (Fixed), Flex, Null Dereference, src/gen.c, mkfttbl, calloc @660, 662
12 (Fixed), Flex, Null Dereference, src/scanopt.c, scanopt_init, malloc @141, 143
13 (Fixed), Flex, Null Dereference, src/scanflags.c, sf_push, realloc @46, 48
14 (Fixed), Flex, Null Dereference, src/misc.c, sko_push, realloc @70, 73
15 (Fixed), Flex, Null Dereference, src/gen.c, mkcttbl, calloc @223, 286
16 (Fixed), Flex, Null Dereference, src/scanopt.c, scanopt_usage, malloc @253, 454
17 (Fixed), Flex, Null Dereference, src/main.c, check_options, calloc @364, 367
18 (Fixed), Flex, Null Dereference, src/scanflags.c, sf_init, malloc @71, 74
19 (Fixed), Flex, Memory Leak, src/buf.c, buf_m4_define, malloc @175, 180

```

```

20 (Fixed), Flex, Memory Leak, src/buf.c, buf_m4_undefine, malloc @196, 202
21 (Fixed), Flex, Memory Leak, src/regex.c, regmatch_strtol, regmatch_dup @143, 147
22 (Fixed), Flex, Memory Leak, src/misc.c, sko_push, malloc @63, 83
23 (Fixed), Flex, Resource Leak, src/filter.c, filter_tee_header, fdopen @245, 249

```

C.5 p11-kit project

```

1 (Fixed), P11, Null Dereference, trust/index.c, index_build, p11_array_new @367, 383
2 (Fixed), P11, Null Dereference, p11-kit/rpc-transport.c, rpc_exec_init, p11_array_new @1045, 1055
3 (Fixed), P11, Null Dereference, rpc-server.c, p11_kit_remote_serive_tokens, p11_array_new @2249, 2266
4 (Fixed), P11, Null Dereference, p11-kit/trust/builder.c, replace_nss_trust_object, p11_array_new @1432,
  1434
5 (Fixed), P11, Memory Leak, trust/save.c, cleanup_directory, p11_dict_new @555, 567
6 (Fixed), P11, Memory Leak, trust/parser.c, load_seq_of_oid_str, p11_dict_new @279, 289
7 (Fixed), P11, Memory Leak, p11-kit/modules.c, managed_track_session_inlock, memdup @1599, 1603
8 (Fixed), P11, Memory Leak, trust/asn1.c, p11_asn1_defs_load, p11_dict_new @75, 84
9 (Fixed), P11, Memory Leak, common/attrs.c, attrs_build, malloc @152, 162
10 (Fixed), P11, Memory Leak, trust/asn1.c, p11_asn1_encode, malloc @179, 187
11 (Fixed), P11, Memory Leak, trust/asn1.c, p11_asn1_read, malloc @215, 219
12 (Fixed), P11, Memory Leak, trust/extract-openssl.c, load_usage_ext, malloc @120, 124
13 (Fixed), P11, Memory Leak, trust/extract-openssl.c, write_keyid, malloc @236, 241
14 (Fixed), P11, Memory Leak, trust/parser.c, p11_parser_new, p11_asn1_defs_load @652, 660
15 (Fixed), P11, Memory Leak, trust/parser.c, p11_parser_new, p11_asn1_defs_load @652, 662
16 (Fixed), P11, Memory Leak, p11-kit/uri.c, parse_string_attribute, p11_url_decode @1278, 1283
17 (Fixed), P11, Memory Leak, p11-kit/filter.c, p11_filter_allow_token, memdup @408, 411
18 (Fixed), P11, Memory Leak, p11-kit/filter.c, p11_filter_deny_token, memdup @428, 431
19 (Fixed), P11, Memory Leak, p11-kit/modules.c, managed_track_session_inlock, memdup @1602, 1608
20 (Fixed), P11, Memory Leak, p11-kit/uri.c, parse_vendor_query, p11_url_decode @1590, 1598
21 (Fixed), P11, Memory Leak, trust/enumerate.c, load_attached_extension, memdup @84, 90
22 (Fixed), P11, Memory Leak, trust/module.c, sys_C_FindObjectsInit, p11_dict_new @1226, 1242
23 (Fixed), P11, Memory Leak, trust/module.c, find_objects_match, memdup @1331, 1338
24 (Fixed), P11, Memory Leak, trust/token.c, p11_token_new, p11_path_build @858, 862, 859, 856, 853
25 (Fixed), P11, Memory Leak, trust/save.c, cleanup_directory, p11_dict_new @555, 562
26 (Fixed), P11, Memory Leak, trust/token.c, loader_load_directory, p11_token_new, p11_dict_new @849, 853
27 (Fixed), P11, Memory Leak, trust/token.c, loader_load_directory, p11_token_new, p11_dict_new @849, 856
28 (Fixed), P11, Memory Leak, trust/token.c, loader_load_directory, p11_token_new, p11_dict_new @849, 859
29 (Fixed), P11, Memory Leak, trust/token.c, loader_load_directory, p11_token_new, p11_dict_new @849, 862
30 (Fixed), P11, Memory Leak, p11-kit/modules.c, managed_track_session_inlock, memdup @1599, 1608
31 (Fixed), P11, Memory Leak, common/attrs.c, attrs_build, memdup @154, 162
32 (Fixed), P11, Resource Leak, trust/token.c, loader_load_directory, opendir @257, 266
33 (Fixed), P11, Resource Leak, p11-kit/conf.c, load_configs_from_directory, opendir @403, 422
34 (Fixed), P11, Resource Leak, trust/save.c, cleanup_directory, opendir @549, 561
35 (Fixed), P11, Resource Leak, trust/save.c, cleanup_directory, opendir @549, 566
36 (Fixed), P11, Resource Leak, p11-kit/rpc-transport.c, rpc_unix_connect, socket @1084, 1096
37 (Fixed), P11, Resource Leak, p11-kit/rpc-transport.c, rpc_unix_connect, socket @1084, 1099

```

C.6 x264 project

```

1 (Fixed), x264, Memory Leak, input/thread.c, open_file, malloc @53, 54
2 (Fixed), x264, Memory Leak, input/thread.c, open_file, malloc @53, 61
3 (Fixed), x264, Memory Leak, filters/video/cache.c, init, malloc @70, 72
4 (Fixed), x264, Memory Leak, filters/video/select_every.c, init, malloc @60, 76
5 (Fixed), x264, Memory Leak, filters/video/select_every.c, init, malloc @60, 75
6 (Fixed), x264, Memory Leak, filters/video/select_every.c, init, malloc @60, 79
7 (Fixed), x264, Memory Leak, filters/video/select_every.c, init, malloc @60, 80
8 (Fixed), x264, Memory Leak, filters/video/select_every.c, init, malloc @60, 83
9 (Fixed), x264, Memory Leak, input/timecode.c, open_file, malloc @347, 384
10 (Fixed), x264, Memory Leak, input/timecode.c, open_file, malloc @347, 371
11 (Fixed), x264, Memory Leak, input/timecode.c, open_file, malloc @347, 376
12 (Fixed), x264, Memory Leak, filters/video/select_every.c, init, malloc @82, 102
13 (Fixed), x264, Memory Leak, output/flv.c, malloc @182, 224
14 (Fixed), x264, Memory Leak, output/flv.c, malloc @182, 222
15 (Fixed), x264, Memory Leak, filters/video/select_every.c, init, malloc @60, 102
16 (Fixed), x264, Memory Leak, filters/video/cache.c, init, malloc @64, 72
17 (Fixed), x264, Resource Leak, input/y4m.c, open_file, fopen @89, 106
18 (Fixed), x264, Resource Leak, input/y4m.c, open_file, fopen @89, 107
19 (Fixed), x264, Resource Leak, input/raw.c, open_file, fopen @79, 102
20 (Fixed), x264, Resource Leak, input/y4m.c, open_file, fopen @89, 194
21 (Fixed), x264, Resource Leak, input/y4m.c, open_file, fopen @89, 195, 222, 230

```

C.7 recutils-1.8 project

1	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-utils.c,	rec_extract_file,	malloc @102,	103
2	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-utils.c,	rec_extract_url,	malloc @130,	131
3	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-utils.c,	rec_extract_type,	malloc @159,	160
4	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-utils.c,	rec_parse_regexp,	malloc @231,	232
5	(Fixed),	recutils-1.8,	Null Dereference,	utils/recfmt.c,	recfmt_get_subst,	rec_sex_new @161,	162
6	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-rset.c,	rec_rset_dup,	malloc @273,	302, 305
7	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-record.c,	rec_record_uniq,	malloc @663,	664
8	(Fixed),	recutils-1.8,	Null Dereference,	utils/recinf.c,	print_info_file,	rec_parser_new @130,	193
9	(Fixed),	recutils-1.8,	Null Dereference,	utils/recutil.c,	recutil_parse_db_from_file,	rec_parser_new @245,	290
10	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-db.c,	rec_db_delete,	rec_db_get_rset_by_type @738,	746
11	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-db.c,	rec_db_set,	rec_db_get_rset_by_type @832,	840
12	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-parser.c,	rec_parse_field_name_str,	rec_parser_new_str @681,	685
13	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-parser.c,	rec_parse_comment,	rec_buf_new @1091,	1117
14	(Fixed),	recutils-1.8,	Null Dereference,	utils/recfix.c,	recfix_check_database,	rec_buf_new @343,	348
15	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-rset.c,	rec_rset_source,	rec_mset_get_at @698,	699
16	(Fixed),	recutils-1.8,	Null Dereference,	lib/obstack.c,	_obstack_newchunk,	call_chunkfun @200,	204
17	(Fixed),	recutils-1.8,	Null Dereference,	utils/recins.c:179,	recins_parse_args,	rec_sex_new @179,	179
18	(Fixed),	recutils-1.8,	Null Dereference,	utils/recdel.c:192,	recdel_parse_args,	rec_sex_new @192,	192
19	(Fixed),	recutils-1.8,	Null Dereference,	utils/recset.c:196,	recset_parse_args,	rec_sex_new @196,	196
20	(Fixed),	recutils-1.8,	Null Dereference,	utils/recsel.c,	recsel_parse_args,	rec_sex_new @199,	199
21	(Fixed),	recutils-1.8,	Null Dereference,	utils/recdel.c,	rec_sex_new @234,	235	
22	(Fixed),	recutils-1.8,	Null Dereference,	lib/wait-process.c,	register_slave_subprocess,	malloc @147,	156
23	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-rset.c,	rec_rset_rename_field,	rec_buf_new @505,	507
24	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-types.c,	rec_type_reg_add,	realloc @769,	777
25	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-types.c,	rec_type_reg_add_synonym,	realloc @808,	810
26	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-record.c,	rec_record_to_comment,	rec_buf_new @432,	450
27	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-record.c,	rec_record_uniq,	malloc @663,	664
28	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-db.c,	rec_db_query,	rec_db_get_rset_by_type @298,	312
29	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-buf.c,	rec_buf_new,	malloc @61,	72
30	(Fixed),	recutils-1.8,	Null Dereference,	src/rec-db.c,	rec_db_set_act_rename,	rec_fex_get @1219,	1220
31	(Fixed),	recutils-1.8,	Memory Leak,	lib/malloca.c,	malloca,	malloc @52,	67
32	(Fixed),	recutils-1.8,	Memory Leak,	lib/time_rz.c,	localtime_rz,	set_tz @308,	311
33	(Fixed),	recutils-1.8,	Memory Leak,	lib/time_rz.c,	mktime_z,	set_tz @327,	342,
34	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-db.c,	rec_db_get_rset_by_type,	rec_rset_type @237,	263,
35	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-db.c,	rec_db_get_rset_by_type,	rec_rset_type @237,	250
36	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-sex-lex.c,	sex_scan_bytes,	sexalloc @2134,	2145
37	(Fixed),	recutils-1.8,	Memory Leak,	utils/recutil.c,	recutil_check_integrity,	rec_buf_new @476,	491
38	(Found but not Fixed),	recutils-1.8,	Memory Leak,	src/rec-sex-lex.c,	sexrestart,	sex_create_buffer @1743,	1733
39	(Found but not Fixed),	recutils-1.8,	Memory Leak,	utils/rec2csv.c,	rec_rset_type @302,	no handler	
40	(Found but not Fixed),	recutils-1.8,	Memory Leak,	utils/rec2csv.c,	rec_rset_type @306,	no handler	
41	(Found but not Fixed),	recutils-1.8,	Memory Leak,	src/rec-mset.c,	rec_mset_add_sorted @256,	no handler	
42	(Fixed),	recutils-1.8,	Memory Leak,	lib/time_rz.c,	localtime_rz,	set_tz @308,	315 (This is correct!)
43	(Fixed),	recutils-1.8,	Memory Leak,	lib/time_rz.c,	mktime_z,	set_tz @327,	340
44	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-sex-lex.c,	sex_scan_bytes,	sexalloc @2134,	2145
45	(Fixed),	recutils-1.8,	Memory Leak,	lib/time_rz.c,	set_tz @308,	315	
46	(Fixed),	recutils-1.8,	Memory Leak,	lib/time_rz.c,	set_tz @308,	313	
47	(Fixed),	recutils-1.8,	Memory Leak,	lib/time_rz.c,	set_tz @327,	342	
48	(Fixed),	recutils-1.8,	Memory Leak,	lib/time_rz.c,	set_tz @327,	340	
49	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-record.c,	rec_record_to_comment,	rec_buf_new @432,	467
50	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-rset.c,	rec_rset_rename_field,	rec_buf_new @505,	515
51	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-rset.c,	rec_rset_group,	malloc @765,	807
52	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-db.c,	rec_db_set_act_delete,	malloc @1375,	1456
53	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-db.c,	rec_db_set_act_delete,	malloc @1375,	1437
54	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-db.c,	rec_db_process_fex,	malloc @1671,	1696
55	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-db.c,	rec_db_process_fex,	malloc @1671,	1687
56	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-parser.c,	rec_parse_field_name,	rec_buf_new @228,	340
57	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-parser.c,	rec_parse_field_name,	rec_buf_new @228,	282
58	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-parser.c,	rec_parse_field_value,	rec_buf_new @924,	1077
59	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-parser.c,	rec_parse_field_value,	1056	
60	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-parser.c,	rec_parse_field_value,	1043	
61	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-parser.c,	rec_parse_field_value,	1028	
62	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-parser.c,	rec_parse_comment,	rec_buf_new @1091,	1136
63	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-parser.c,	rec_parse_comment,	rec_buf_new @1091,	1121
64	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-sex-lex.c,	sex_create_buffer,	sexalloc @1824,	1835
65	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-sex-lex.c,	sex_create_buffer,	sexalloc @1824,	2041
66	(Fixed),	recutils-1.8,	Memory Leak,	src/rec-fex.c,	rec_fex_str,	rec_buf_new @353,	414

67 (Fixed), recutils-1.8, Memory Leak, src/rec-fex.c, rec_fex_str, rec_buf_new @353, 377
 68 (Fixed), recutils-1.8, Memory Leak, src/rec-types.c, rec_type_check, rec_buf_new @583, 675
 69 (Fixed), recutils-1.8, Memory Leak, utils/recutl.c, recutl_parse_db_from_file, rec_rset_type @250, 298, 254
 70 (Fixed), recutils-1.8, Memory Leak, utils/recfix.c, recfmt_apply_template, rec_buf_new @207, 250
 71 (Fixed), recutils-1.8, Resource Leak, utils/csv2rec.c, process_csv, fopen @345, 383
 72 (Fixed), recutils-1.8, Resource Leak, utils/recutl.c, recutl_read_db_from_file, fopen @363, 384
 73 (Fixed), recutils-1.8, Resource Leak, utils/recutl.c, recutl_write_db_to_file, fdopen @419, 438
 74 (Fixed), recutils-1.8, Resource Leak, utils/recutl.c, recutl_write_db_to_file, fdopen @419, 428
 75 (Fixed), recutils-1.8, Resource Leak, src/rec-int.c, rec_int_merge_remote, fdopen @1148, 1251
 76 (Fixed), recutils-1.8, Resource Leak, src/rec-int.c, rec_int_merge_remote, fdopen @1172, 1251
 77 (Fixed), recutils-1.8, Resource Leak, utils/csv2rec.c, process_csv, fopen @345, 359,
 78 (Fixed), recutils-1.8, Resource Leak, utils/csv2rec.c, process_csv, fopen @345, 377

C.8 inetutils-1.9.4 project

1 (Fixed), inetutils, Null Dereference, lib/obstack.c, _obstack_newchunk, call_chunkfun @200, 222
 2 (Fixed), inetutils, Null Dereference, ifconfig/printif.c, put_addr, strchr @279, 281
 3 (Fixed), inetutils, Null Dereference, ifconfig/printif.c, put_addr, strchr @284, 285
 4 (Fixed), inetutils, Null Dereference, ifconfig/printif.c, put_addr, strchr @288, 289
 5 (Fixed), inetutils, Null Dereference, src/hostname.c, get_name, get_name_action @174, 210
 6 (Fixed), inetutils, Null Dereference, libinetutils/ttymsg.c, normalize_path, strchr @273, 275
 7 (Fixed), inetutils, Null Dereference, src/tftp.c, put, strchr @622, 623
 8 (Fixed), inetutils, Null Dereference, src/tftp.c, put, strchr @588, 589
 9 (Fixed), inetutils, Null Dereference, ftp/cmds.c, setnmap, strchr @2295, 2302
 10 (Fixed), inetutils, Null Dereference, ftp/cmds.c, setnmap, strchr @2289, 2297
 11 (Fixed), inetutils, Null Dereference, ping/ping-common.c, sinaddr2str, inet_ntoa @319, 320
 12 (Fixed), inetutils, Null Dereference, ifconfig/printif.c, put_addr, inet_ntoa @293, 302
 13 (Fixed), inetutils, Null Dereference, ifconfig/printif.c, put_addr, inet_ntoa @277, 291
 14 (Fixed), inetutils, Memory Leak, libinetutils/ttymsg.c, ttymsg, malloc @87, 113
 15 (Fixed), inetutils, Memory Leak, libinetutils/ttymsg.c, ttymsg, malloc @87, 102
 16 (Fixed), inetutils, Memory Leak, libinetutils/ttymsg.c, ttymsg, malloc @87, 155
 17 (Fixed), inetutils, Memory Leak, libinetutils/argcv.c, argv_string, malloc @149, 175
 18 (Fixed), inetutils, Memory Leak, ftp/cmds.c, remglob, malloc @1088, 1110
 19 (Fixed), inetutils, Memory Leak, ping/ping6.c, send_echo, ping_set_data @442, 446
 20 (Fixed), inetutils, Memory Leak, ping/ping6.c, send_echo, ping_set_data @438, 450
 21 (Fixed), inetutils, Memory Leak, lib/fnmatch.c, posix_fnmatch, malloc @310, 314
 22 (Fixed), inetutils, Memory Leak, lib/fnmatch.c, posix_fnmatch, malloc @310, 329
 23 (Fixed), inetutils, Memory Leak, telnet/telnet.c, mklst, malloc @656, 751
 24 (Fixed), inetutils, Memory Leak, ftp/ftp.c, gunique, malloc @1916, 1936
 25 (Fixed), inetutils, Memory Leak, ftp/ftp.c, gunique, malloc @1916, 1947
 26 (Fixed), inetutils, Memory Leak, ftp/ftp.c, gunique, malloc @1916, 1933
 27 (Fixed), inetutils, Memory Leak, lib/glob.c, glob_in_dir, malloc @1468, 1554
 28 (Fixed), inetutils, Memory Leak, lib/glob.c, glob_in_dir, malloc @1452, 1554
 29 (Fixed), inetutils, Memory Leak, ping/ping.c, send_echo, ping_set_data @514, 522
 30 (Fixed), inetutils, Memory Leak, ping/ping.c, send_echo, ping_set_data @511, 522
 31 (Fixed), inetutils, Resource Leak, libls/fts.c, fts_children, rpl_open @601, 606
 32 (Fixed), inetutils, Resource Leak, src/tftp.c, put, rpl_open @607, 618
 33 (Fixed), inetutils, Resource Leak, src/tftp.c, put, rpl_open @627, 633
 34 (Fixed), inetutils, Resource Leak, ftp/cmds.c, remglob, fopen @1078, 1107
 35 (Fixed), inetutils, Resource Leak, ftp/cmds.c, remglob, fopen @1078, 1110
 36 (Fixed), inetutils, Resource Leak, ftp/cmds.c, remglob, fopen @1078, 1096

C.9 snort-2.9.13 project

1 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/appid/thirdparty_appid_utils.c, getXffFields, malloc @99, 104
 2 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/perf.c, sfRotateFile, localtime @287, 289
 3 (Fixed), snort-2.9.13, Null Dereference, src/util.c, gm2local, localtime @311, 313
 4 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/Session/session-common.c, registerDirectionPortCallback, getSessionPlugins @109, 114, 112
 5 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/Session/session-common.c, registerFlushStreamCallback, getSessionPlugins @121, 126, 124
 6 (Fixed), snort-2.9.13, Null Dereference, Frag3ReloadVerify, sfPolicyUserDataGetDefault @5077, 5086
 7 (Fixed), snort-2.9.13, Null Dereference, Frag3ReloadVerify, sfPolicyUserDataGetDefault @5076, 5086
 8 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_frag3.c, Frag3CleanExit, sfPolicyUserDataGetDefault @4456, 4459
 9 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_frag3.c, Frag3MemReloadAdjust, sfPolicyUserDataGetCurrent @4963, 4966

10 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/ssl_common/ssl_inspect.c, SSLPP_is_encrypted, sfPolicyUserDataGetCurrent @342, 344

11 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/smtp/snort_smtp.c, SMTP_GetNewSession, sfPolicyUserDataGetCurrent @361, 363

12 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/reputation/spp_reputation.c, ReputationReloadSwap, sfPolicyUserDataGetDefault @1074, 1075

13 (Fixed), snort-2.9.13, Null Dereference, src/sfutil/acsmx.c, acsmAddPattern, AC_MALLLOC @484, 487

14 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/Stream6/snort_stream_tcp.c, StreamTcpPolicyClone, sfPolicyUserDataGet @1458, 1459

15 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/ssl_common/ssl_inspect.c, SSLPP_process_alert, sfPolicyUserDataGetCurrent @378, 389

16 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/ssl_common/ssl_inspect.c, SSLPP_process_app, sfPolicyUserDataGetCurrent @433, 437

17 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_stream6.c, initStreamPolicyConfig, sfPolicyConfigCreate @351, 378

18 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/ssl_common/ssl_inspect.c, SSLPP_process_other, sfPolicyUserDataGetCurrent @470, 476

19 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/sdf/spp_sdf.c, ProcessSDF, sfPolicyUserDataGetCurrent @517, 550

20 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_arpspoof.c, ARPsPoofReload, sfPolicyConfigCreate @713, 714

21 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_normalize.c, Reload_GetContext, sfPolicyConfigCreate @776, 780

22 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_bo.c, BoReload, sfPolicyConfigCreate @891, 892

23 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/Stream6/stream_common.c, StreamActiveResponse, sfPolicyUserDataGet @146, 147

24 (Fixed), snort-2.9.13, Null Dereference, src/fpdetect.c, fpAddMatch, getRuntimeRtnFromOtn @423, 425

25 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/pop/spp_pop.c, POPCheckConfig, sfPolicyUserDataGetDefault @510, 534

26 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/pop/spp_pop.c, POPReloadVerify, sfPolicyUserDataGet @758, 776

27 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/imap/spp_imap.c, IMAPReloadVerify, sfPolicyUserDataGet @762, 779

28 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/ftptelnet/pp_ftp.c, initialize_ftp, sfPolicyUserDataGet @942, 957

29 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/reputation/spp_reputation.c, ReputationCheckConfig, sfPolicyUserDataGetDefault @864, 866

30 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/reputation/spp_reputation.c, ReputationCheckConfig, sfPolicyUserDataGetDefault @864, 866

31 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_frag3.c, Frag3ReloadGlobal, sfPolicyConfigCreate @4809, 4810

32 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/smtp/spp_smtp.c, SMTPReloadVerify, sfPolicyUserDataGet @788, 805

33 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/imap/spp_imap.c, POPReloadSwap, sfPolicyUserDataGet @842, 856

34 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_arpspoof.c, ARPsPoofInit, sfPolicyUserDataGetCurrent @216, 243

35 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_arpspoof.c, ARPsPoofInit, sfPolicyConfigCreate @205, 214

36 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_arpspoof.c, ARPsPoofHostInit, sfPolicyUserDataGetCurrent @284, 295

37 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_arpspoof.c, ARPsPoofReload, sfPolicyUserDataGetCurrent @719, 739

38 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_arpspoof.c, ARPsPoofReloadHost, sfPolicyUserDataGetCurrent @764, 769

39 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_bo.c, BoInit, sfPolicyConfigCreate @252, 266

40 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_rpc_decode.c, RpcDecodeInit, sfPolicyConfigCreate @277, 296

41 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_rpc_decode.c, RpcDecodeReload, sfPolicyConfigCreate @1461, 1462

42 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_httpinspect.c, HttpInspectInit, sfPolicyConfigCreate @586, 587

43 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_httpinspect.c, HttpInspectReloadSwap, sfPolicyUserDataGetDefault @2147, 2179

44 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_sfportscan.c, PortscanInit, sfPolicyUserDataGetCurrent @1248, 1268

45 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_sfportscan.c, PortscanInit, sfPolicyConfigCreate @1228, 1247

46 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_sfportscan.c, PortscanReload, sfPolicyUserDataGetCurrent @1536, 1563

47 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_sfportscan.c, PortscanReload, sfPolicyConfigCreate @1523, 1524

48 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_frag3.c, Frag3GlobalInit, sfPolicyUserDataGetDefault @1120, 1142

49 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_frag3.c, Frag3GlobalInit, sfPolicyUserDataGetCurrent @1119, 1138

50 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_frag3.c, Frag3GlobalInit, sfPolicyConfigCreate @1097, 1118

51 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_frag3.c, Frag3ReloadGlobal, sfPolicyUserDataGetCurrent @4815, 4833

52 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_frag3.c, Frag3ReloadGlobal, sfPolicyUserDataGetDefault @4814, 4836

53 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_stream6.c, initStreamPolicyConfig, sfPolicyUserDataGetCurrent @379, 386

54 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_normalize.c, Init_GetContext, sfPolicyUserDataGetCurrent @125, 131

55 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_normalize.c, Init_GetContext, sfPolicyConfigCreate @118, 122

56 (Fixed), snort-2.9.13, Null Dereference, src/preprocessors/spp_normalize.c, Reload_GetContext, sfPolicyUserDataGetCurrent @783, 790

57 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/pop/snort_pop.c, POP_GetNewSession, sfPolicyUserDataGetCurrent @283, 349

58 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/imap/snort_imap.c, IMAP_GetNewSession, sfPolicyUserDataGetCurrent @325, 392

59 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/imap/spp_imap.c, IMAPReloadSwap, sfPolicyUserDataGet @850, 870

60 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/smtp/snort_smtp.c, SMTPReloadSwap, sfPolicyUserDataGet @867, 886

61 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/dcerpc2/spp_dce2.c, DCE2_InitGlobal, sfPolicyConfigCreate @224, 300

62 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/dcerpc2/spp_dce2.c, DCE2_InitServer, sfPolicyUserDataGetCurrent @373, 377

63 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/dcerpc2/spp_dce2.c, DCE2_ReloadGlobal, sfPolicyConfigCreate @1056, 1067

64 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/dcerpc2/spp_dce2.c, DCE2_ReloadServer, sfPolicyUserDataGetCurrent @1146, 1150

65 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/sdf/sdf_us_ssn.c, ParseSSNGroups, malloc @195, 201

66 (Fixed), snort-2.9.13, Null Dereference, src/dynamic-preprocessors/sip/spp_sip.c, IPReloadVerify, sfPolicyUserDataGet @977, 991

67 (Fixed), snort-2.9.13, Null Dereference, dynamic-preprocessors/appid/service_plugins/service_rtmp.c, parse_rtmp_message, malloc @348, 413

68 (Fixed), snort-2.9.13, Memory Leak, appid/detector_plugins/http_url_patterns.c, addMlmpPattern, malloc @93, 162

69 (Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/sip/sip_roptions.c, SIP_MethodInit, SIP_AddUserDefinedMethod @149, 175

70 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/detector_plugins/detector_pop3.c, pop3_ca_init, AppIdAddGenericConfigItem @260, no handler, fix should be in 282, 293

71 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/detector_plugins/detector_imap.c, init, AppIdAddGenericConfigItem @296, no handler, fix should be in 319, 330

72 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/service_plugins/service_ssl.c, ssl_validate, parse_client_initiation @581, no handler

73 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/luadetectorapi.c, service_addPorts, ServiceAddPort @926, no handler

74 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/luadetectorapi.c, ClientAppRegisterPattern @1793, no handler

75 (Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/luadetectorapi.c, Detector_addRTMPUrl, malloc @3267, 3306

76 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/luadetectorapi.c, Detector_addSipUserAgent, sipUaPatternAdd @3357, no handler

77 (Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/luadetectorapi.c, openAddUrlPattern, malloc @3670, 3706

78 (Found but not Fixed), snort-2.9.13, Memory Leak, src/preprocessors/spp_stream6.cStreamProcess, updateMplsHeaders @911, no handler, 920,

79 (Found but not Fixed), snort-2.9.13, Memory Leak, src/preprocessors/spp_stream6.cStreamProcess, updateMplsHeaders @911, no handler, 928,

80 (Found but not Fixed), snort-2.9.13, Memory Leak, src/preprocessors/spp_stream6.cStreamProcess, updateMplsHeaders @911, no handler, 939,

81 (Found but not Fixed), snort-2.9.13, Memory Leak, src/preprocessors/spp_stream6.cStreamProcess, updateMplsHeaders @911, no handler ,945,

82 (Found but not Fixed), snort-2.9.13, Memory Leak, src/preprocessors/spp_stream6.cStreamProcess, updateMplsHeaders @911, no handler ,948,

83 (Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/luadetectorapi.c, Detector_addAppUrl, malloc @3120, 3158

84 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/luadetectorapi.c, Detector_addSipServer, sipServerPatternAdd @4011, no handler

85 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/client_plugins/client_app_base.c, CClientAppRegisterPattern, ClientAppRegisterPattern @240, no handler

86 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/client_plugins/client_app_base.c, CClientAppRegisterPatternNoCase, ClientAppRegisterPattern @247, no handler

87 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/client_plugins/client_app_base.c, LuaClientAppRegisterPattern, ClientAppRegisterPattern @254, no handler

88 (Fixed), snort-2.9.13, Memory Leak, dynamic-preprocessors/appid/service_plugins/service_base.c, AppIdAddDHCP, malloc @1177, 1195

89 (Fixed), snort-2.9.13, Memory Leak, dynamic-preprocessors/appid/service_plugins/service_base.c, AppIdAddDHCP, malloc @1177, 1184

90 (Fixed), snort-2.9.13, Memory Leak, dynamic-preprocessors/appid/service_plugins/service_base.c, AppIdAddSMBData, malloc @1269, 1282

91 (Fixed), snort-2.9.13, Memory Leak, dynamic-preprocessors/appid/service_plugins/service_base.c, AppIdAddSMBData, malloc @1269, 1276

92 (Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/service_plugins/service_ssh.c, ssh_validate, malloc @510, 511

93 (Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/service_plugins/service_ssh.c, ssh_validate, malloc @510, 514

94 (Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/service_plugins/service_ssh.c, ssh_validate, malloc @499, 511

95 (Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/service_plugins/service_ssh.c, ssh_validate, malloc @499, 514

96 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/service_plugins/service_ssh.c, ssh_validate, malloc @523, 524

97 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/service_plugins/service_ssh.c, ssh_validate, malloc @523, 527

98 (Found but not Fixed), snort-2.9.13, Memory Leak, src/dynamic-preprocessors/appid/service_plugins/service_MDNS.c, mdnsMatcherCreate, 'AppIdAddGenericConfigItem @487, no handler

99 (Fixed), snort-2.9.13, Resource Leak, src/output-plugins/spo_unified2.c, Unified2PostConfig, Unified2InitFile @274, 276

100 (Fixed), snort-2.9.13, Resource Leak, src/output-plugins/spo_unified2.c, Unified2RotateFile, Unified2InitFile @355, 351

C.10 grub project

1 (Fixed), Grub, Null Dereference, grub-core/efiemu/symbols.c, grub_efiemu_write_value, grub_efiemu_mm_obtain_request @154, 262

2 (Fixed), Grub, Null Dereference, grub-core/tests/lib/test.c, grub_test_assert_helper, failure_start @168, 173

3 (Fixed), Grub, Null Dereference, grub-core/efiemu/symbols.c, grub_efiemu_write_sym_markers, grub_efiemu_mm_obtain_request @134, 137

4 (Fixed), Grub, Null Dereference, grub-core/efiemu/symbols.c, grub_efiemu_write_value, grub_efiemu_mm_obtain_request @154, 165

5 (Fixed), Grub, Null Dereference, grub-core/efiemu/symbols.c, grub_efiemu_set_virtual_address_map, grub_efiemu_mm_obtain_request @221, 227

6 (Fixed), Grub, Null Dereference, grub-core/fs/proc.c, grub_procfs_open, grub_procfs_rewind @160, 165

7 (Fixed), Grub, Null Dereference, grub/grub-core/efiemu/pnvr.am.c, nvram_set, grub_efiemu_mm_obtain_request @103, 113

8 (Fixed), Grub, Null Dereference, grub/grub-core/efiemu/pnvr.am.c, nvram_set, grub_efiemu_mm_obtain_request @101, 115

9 (Fixed), Grub, Null Dereference, grub/grub-core/efiemu/pnvr.am.c, nvram_set, grub_efiemu_mm_obtain_request @99, 111

10 (Fixed), Grub, Null Dereference, nvram_set, grub_efiemu_mm_obtain_request @97, 111

11 (Fixed), Grub, Null Dereference, nvram_set, grub_efiemu_mm_obtain_request @95, 203

12 (Fixed), Grub, Memory Leak, grub-core/gnulib/localcharset.c, get_charset_aliases, malloc @219, 344

D DOUBLE FREE

Here are the detailed bug records shown in Table. 4. In particular, there are two false positives produced by PROVENFIX.

```

1 (Fixed, more ture bug 1), P11, Double Free, trust/extract.c, p11_trust_extract_compat, free @323, 329
2 (Fixed), P11, Double Free, trust/extract.c, p11_trust_extract_compat, free @ 316, 329
3 (Fixed), P11, Double Free, p11-kit/server.c, main, free @ 790, 798
4 (False Positive), P11, Double Free, p11-kit/p11-kit/client.c, C_GetFunctionList, free @ 136, 142
5 (Fixed), Grub, Double Free, grub-core/io/lzopio.c, grub_script_lexer_init, yylex_destroy @ 253, 254
6 (Fixed, more ture bug 2), Grub, Double Free, grub-core/io/lzopio.c, test_header, grub_free @ 377, 390
7 (Fixed), Grub, Double Free, grub-core/io/lzopio.c, test_header, grub_free @ 370, 406
8 (False Positive), Grub, Double Free, grub-core/fs/archelp.c, grub_archelp_dir , grub_free @199 // cause
   by unrolling once loop

```

More True Bug 1: In project p11-kit, (commit cdf540c, function "p11_trust_extract_compat"), SAVER recorded the double free on lines (316,329) but missed out on the one on (323,329). The fix provided by the developer was to remove the free statement on line 329, which happens to solve both bugs.

More True Bug 2: In project Grub (commit 9e34a34, function "test_header"), SAVER recorded the double free on lines (370,406) but missed out on the one on (377,406). The fix provided by the developer was to remove the free statement on line 406, which happens to solve both bugs, but the bug shown on (377,406) seems to have never been spotted/recorded by people.

PROVENFIX False Positive 1: As shown in Fig. 1, the false positive is recognized due to the free statement in line 7 and the dereference of "state" in line 12. However, this is not a true bug because lines 7 and 12 will never be executed in sequence due to the reassignment at line 8.

```

1 CK_RV C_GetFunctionList (CK_FUNCTION_LIST_PTR_PTR list)
2 {
3     ...
4     rv = get_server_address (&address);
5     if (rv == CKR_OK) {
6         module = p11_virtual_wrap (...);
7         if (!module) {
8             free (state); // the free statement
9             rv = CKR_GENERAL_ERROR; // due to this re-assignment
10        }
11    }
12    if (rv == CKR_OK) {
13        state->wrapped = module; // false positive double free
14    }
15 }

```

Fig. 1. False positive in p11.

PROVENFIX False Positive 2: As shown in Fig. 2, the false positive is recognized due to the first free statement in line 10, and the second free statement of "state" in line 18. However, this is not a true bug because 1) lines 10 and 18 will never be executed in sequence due to the while(1) statement at line 4 and 2) the aliasing at line 11. This example shows the limitation of PROVENFIX's analysis, i.e., unrolling loops only once, and limited capability for complex aliasing.

E INFERRED SPECS FOR OPENSSL APIS

To infer future-condition specs for OpenSSL APIs, we deploy the first primitive spec: `ERR_new(); // post: true \wedge ERR()`. Using this spec, for each procedure `nm`, we generate `nm`'s postcondition. If the postcondition contains the event `ERR()`, we generate a future-condition for `nm` which is associated with the return value on the path which triggers the `ERR()` event. It takes PROVENFIX 143.11 seconds to generate future-conditions for 127 OpenSSL APIs, which will be exposed as a library API. Together with these 127 specs, we add the second primitive spec: `return(arg); // post: true \wedge return(arg)`, and use them to analyze and repair OpenSSL applications.

Therefore, all in all, we have manually written two specs and managed to analyze and repair the bugs shown in Table 5. The inferred API specs are shown as follows:

```

1 i2a_ASN1_OBJECT(bp, a); // future: ((ret=-1)  $\wedge$  return(ret))

```

```

1  grub_err_t grub_archelp_dir (...){
2  ...
3  prev = 0;
4  while (1)
5  {
6  if (...) goto fail;
7  if (...) break;
8  canonicalize (name);
9  if (...){
10     grub_free (prev); // the first free statement
11     prev = name; // due to this aliasing
12     ...
13     }
14     else
15     grub_free (name);
16 }
17 fail:
18 grub_free (prev); // false positive, the second free statement
19 return grub_errno;
20 }

```

Fig. 2. False positive in Grub.

```

2  BIO_new_NDEF(out, val, it); // future: ((ret=0) ^ return(ret))
3  BIO_ADDR_new(); // future: ((ret=0) ^ return(ret))
4  BIO_parse_hostserv(hostserv, host, service, hostserv_prio); // future: ((ret=0) ^ return(
   ret))
5  BIO_lookup_ex(host, service, lookup_type, family, socktype, protocol, res); // future: ((
   ret=0) ^ return(ret))
6  BIO_new_ex(libctx, method); // future: ((ret=0) ^ return(ret))
7  BIO_new(method); // future: ((ret=0) ^ return(ret))
8  BIO_gets(b, buf, size); // future: ((ret=-1) ^ return(ret))
9  BIO_get_line(bio, buf, size); // future: ((ret=-1) ^ return(ret))
10 BIO_ctrl(b, cmd, larg, parg); // future: ((ret=-2) ^ return(ret))
11 BIO_callback_ctrl(b, cmd, fp); // future: ((ret=-2) ^ return(ret))
12 BIO_find_type(bio, type); // future: ((ret=0) ^ return(ret))
13 BIO_get_new_index(); // future: ((ret=-1) ^ return(ret))
14 BIO_meth_new(type, name); // future: ((ret=0) ^ return(ret))
15 BIO_sock_info(sock, type, info); // future: ((ret=0) ^ return(ret))
16 BIO_socket(domain, socktype, protocol, options); // future: ((ret=-1) ^ return(ret))
17 BIO_connect(sock, addr, options); // future: ((ret=0) ^ return(ret))
18 BIO_bind(sock, addr, options); // future: ((ret=0) ^ return(ret))
19 BIO_listen(sock, addr, options); // future: ((ret=0) ^ return(ret))
20 BIO_accept_ex(accept_sock, addr_, options); // future: ((ret=-1) ^ return(ret))
21 BIO_ACCEPT_new(); // future: ((ret=0) ^ return(ret))
22 BIO_ctrl_get_write_guarantee(bio); // future: ((ret=-2) ^ return(ret))
23 BIO_ctrl_get_read_request(bio); // future: ((ret=-2) ^ return(ret))
24 BIO_nread0(bio, buf); // future: ((ret=-2) ^ return(ret))
25 BIO_nread(bio, buf, num); // future: ((ret=-2) ^ return(ret))
26 BIO_nwrite0(bio, buf); // future: ((ret=-2) ^ return(ret))
27 BIO_nwrite(bio, buf, num); // future: ((ret=-2) ^ return(ret))
28 BIO_CONNECT_new(); // future: ((ret=0) ^ return(ret))
29 BIO_new_file(filename, mode); // future: ((ret=0) ^ return(ret))
30 BIO_new_mem_buf(buf, len); // future: ((ret=0) ^ return(ret))
31 BN_usub(r, a, b); // future: ((ret=0) ^ return(ret))
32 BN_BLINDING_new(A, Ai, mod); // future: ((ret=0) ^ return(ret))
33 BN_BLINDING_convert_ex(n, r, b, ctx); // future: ((ret=0) ^ return(ret))
34 BN_BLINDING_invert_ex(n, r, b, ctx); // future: ((ret=0) ^ return(ret))
35 BN_bn2dec(a); // future: ((ret=0) ^ return(ret))
36 BN_hex2bn(bn, a); // future: ((ret=0) ^ return(ret))
37 BN_CTX_new_ex(ctx); // future: ((ret=0) ^ return(ret))
38 BN_CTX_new(); // future: ((ret=0) ^ return(ret))
39 BN_CTX_get(ctx); // future: ((ret=0) ^ return(ret))
40 BN_STACK_push(st, idx); // future: ((ret=0) ^ return(ret))
41 BN_POOL_get(p, flag); // future: ((ret=0) ^ return(ret))
42 BN_div(dv, rm, num, divisor, ctx); // future: ((ret=0) ^ return(ret))

```

```

43 BN_exp(r, a, p, ctx); // future: ((ret=0) /\ return(ret))
44 BN_mod_exp_recp(r, a, p, m, ctx); // future: ((ret=0) /\ return(ret))
45 BN_mod_exp_mont(rr, a, p, m, ctx, in_mont); // future: ((ret=0) /\ return(ret))
46 BN_mod_exp_mont_word(rr, a, p, m, ctx, in_mont); // future: ((ret=0) /\ return(ret))
47 BN_mod_exp_simple(r, a, p, m, ctx); // future: ((ret=0) /\ return(ret))
48 BN_mod_exp2_mont(rr, a1, p1, a2, p2, m, ctx, in_mont); // future: ((ret=0) /\ return(ret))
49 BN_GF2m_mod(r, a, p); // future: ((ret=0) /\ return(ret))
50 BN_new(); // future: ((ret=0) /\ return(ret))
51 BN_GENCB_new(); // future: ((ret=0) /\ return(ret))
52 BN_mod_sqr(r, a, m, ctx); // future: ((ret=0) /\ return(ret))
53 BN_mod_lshift_quick(r, a, n, m); // future: ((ret=0) /\ return(ret))
54 BN_MONT_CTX_new(); // future: ((ret=0) /\ return(ret))
55 BN_mpi2bn(d, n, ain); // future: ((ret=0) /\ return(ret))
56 BN_generate_prime_ex2(ret, bits, safe, add, rem, cb, ctx); // future: ((ret=0) /\ return(
    ret))
57 BN_RECP_CTX_new(); // future: ((ret=0) /\ return(ret))
58 BN_lshift(r, a, n); // future: ((ret=0) /\ return(ret))
59 BN_rshift(r, a, n); // future: ((ret=0) /\ return(ret))
60 BIO_new_CMS(out, cms); // future: ((ret=0) /\ return(ret))
61 BIO_new_PKCS7(out, p7); // future: ((ret=0) /\ return(ret))
62 SSL_dup_CA_list(sk); // future: ((ret=0) /\ return(ret))
63 SSL_CIPHER_description(cipher, buf, len); // future: ((ret=0) /\ return(ret))
64 SSL_COMP_add_compression_method(id, cm); // future: ((ret=1) /\ return(ret))
65 SSL_CONF_cmd(cctx, cmd, value); // future: ((ret=-2) /\ return(ret))
66 SSL_clear(s); // future: ((ret=0) /\ return(ret))
67 SSL_CTX_set_ssl_version(ctx, meth); // future: ((ret=0) /\ return(ret))
68 SSL_new(ctx); // future: ((ret=0) /\ return(ret))
69 SSL_CTX_set_session_id_context(ctx, sid_ctx, sid_ctx_len); // future: ((ret=0) /\ return(
    ret))
70 SSL_set_session_id_context(ssl, sid_ctx, sid_ctx_len); // future: ((ret=0) /\ return(ret))
71 SSL_dane_enable(s, basedomain); // future: ((ret=-1) /\ return(ret))
72 SSL_set_wfd(s, fd); // future: ((ret=0) /\ return(ret))
73 SSL_set_rfd(s, fd); // future: ((ret=0) /\ return(ret))
74 SSL_CTX_check_private_key(ctx); // future: ((ret=0) /\ return(ret))
75 SSL_check_private_key(ssl); // future: ((ret=0) /\ return(ret))
76 SSL_accept(s); // future: ((ret=-1) /\ return(ret))
77 SSL_connect(s); // future: ((ret=-1) /\ return(ret))
78 SSL_read(s, buf, num); // future: ((ret=-1) /\ return(ret))
79 SSL_read_early_data(s, buf, num, readbytes); // future: ((ret=0) /\ return(ret))
80 SSL_peek(s, buf, num); // future: ((ret=-1) /\ return(ret))
81 SSL_sendfile(s, fd, offset, size, flags); // future: ((ret=-1) /\ return(ret))
82 SSL_write(s, buf, num); // future: ((ret=-1) /\ return(ret))
83 SSL_write_early_data(s, buf, num, written); // future: ((ret=0) /\ return(ret))
84 SSL_shutdown(s); // future: ((ret=-1) /\ return(ret))
85 SSL_key_update(s, updatetype); // future: ((ret=0) /\ return(ret))
86 SSL_CTX_set_cipher_list(ctx, str); // future: ((ret=0) /\ return(ret))
87 SSL_set_cipher_list(s, str); // future: ((ret=0) /\ return(ret))
88 SSL_CTX_set_alpn_protos(ctx, protos, protos_len); // future: ((ret=1) /\ return(ret))
89 SSL_set_alpn_protos(ssl, protos, protos_len); // future: ((ret=1) /\ return(ret))
90 SSL_CTX_new_ex(libctx, propq, meth); // future: ((ret=0) /\ return(ret))
91 SSL_CTX_new(meth); // future: ((ret=0) /\ return(ret))
92 SSL_CTX_use_psk_identity_hint(ctx, identity_hint); // future: ((ret=0) /\ return(ret))
93 SSL_use_psk_identity_hint(s, identity_hint); // future: ((ret=0) /\ return(ret))
94 SSL_set_ct_validation_callback(s, callback, arg); // future: ((ret=0) /\ return(ret))
95 SSL_CTX_set_ct_validation_callback(ctx, callback, arg); // future: ((ret=0) /\ return(ret)
    )
96 SSL_CTX_enable_ct(ctx, validation_mode); // future: ((ret=0) /\ return(ret))
97 SSL_enable_ct(s, validation_mode); // future: ((ret=0) /\ return(ret))
98 SSL_client_hello_get1_extensions_present(s, out, outlen); // future: ((ret=0) /\ return(
    ret))
99 SSL_verify_client_post_handshake(ssl); // future: ((ret=0) /\ return(ret))
100 SSL_set0_tmp_dh_pkey(s, dhpkey); // future: ((ret=0) /\ return(ret))
101 SSL_CTX_set0_tmp_dh_pkey(ctx, dhpkey); // future: ((ret=0) /\ return(ret))

```

```

102 SSL_use_certificate(ssl, x); // future: ((ret=0) /\ return(ret))
103 SSL_use_certificate_ASN1(ssl, d, len); // future: ((ret=0) /\ return(ret))
104 SSL_use_PrivateKey(ssl, pkey); // future: ((ret=0) /\ return(ret))
105 SSL_use_PrivateKey_ASN1(type, ssl, d, len); // future: ((ret=0) /\ return(ret))
106 SSL_CTX_use_certificate(ctx, x); // future: ((ret=0) /\ return(ret))
107 SSL_CTX_use_certificate_ASN1(ctx, len, d); // future: ((ret=0) /\ return(ret))
108 SSL_CTX_use_PrivateKey(ctx, pkey); // future: ((ret=0) /\ return(ret))
109 SSL_CTX_use_PrivateKey_ASN1(type, ctx, d, len); // future: ((ret=0) /\ return(ret))
110 SSL_CTX_use_serverinfo_ex(ctx, version, serverinfo, serverinfo_length); // future: ((ret
    =0) /\ return(ret))
111 SSL_CTX_use_serverinfo(ctx, serverinfo, serverinfo_length); // future: ((ret=0) /\ return(
    ret))
112 SSL_use_RSAPrivateKey(ssl, rsa); // future: ((ret=0) /\ return(ret))
113 SSL_use_RSAPrivateKey_ASN1(ssl, d, len); // future: ((ret=0) /\ return(ret))
114 SSL_CTX_use_RSAPrivateKey(ctx, rsa); // future: ((ret=0) /\ return(ret))
115 SSL_CTX_use_RSAPrivateKey_ASN1(ctx, d, len); // future: ((ret=0) /\ return(ret))
116 SSL_SESSION_new(); // future: ((ret=0) /\ return(ret))
117 SSL_SESSION_set1_id(s, sid, sid_len); // future: ((ret=0) /\ return(ret))
118 SSL_SESSION_set1_id_context(s, sid_ctx, sid_ctx_len); // future: ((ret=0) /\ return(ret))
119 SSL_set_session_ticket_ext(s, ext_data, ext_len); // future: ((ret=0) /\ return(ret))
120 SSL_SESSION_print_fp(fp, x); // future: ((ret=0) /\ return(ret))
121 SSL_CTX_set_tlsext_max_fragment_length(ctx, mode); // future: ((ret=0) /\ return(ret))
122 SSL_set_tlsext_max_fragment_length(ssl, mode); // future: ((ret=0) /\ return(ret))
123 SSL_CTX_set_client_cert_engine(ctx, e); // future: ((ret=0) /\ return(ret))
124 BIO_lookup(host, service, lookup_type, family, socktype, res); // future: ((ret=0) /\
    return(ret))
125 BIO_int_ctrl(b, cmd, larg, iarg); // future: ((ret=-2) /\ return(ret))
126 BN_BLINDING_convert(n, b, ctx); // future: ((ret=0) /\ return(ret))
127 BN_BLINDING_invert(n, b, ctx); // future: ((ret=0) /\ return(ret))

```

REFERENCES

- [1] Thomas Reinbacher, Jörg Brauer, Martin Horauer, Andreas Steininger, and Stefan Kowalewski. 2011. Past Time LTL Runtime Verification for Microcontroller Binary Code. In *Formal Methods for Industrial Critical Systems - 16th International Workshop, FMICS 2011, Trento, Italy, August 29-30, 2011. Proceedings (Lecture Notes in Computer Science, Vol. 6959)*, Gwen Salaün and Bernhard Schätz (Eds.). Springer, 37–51. https://doi.org/10.1007/978-3-642-24431-5_5
- [2] César Sánchez and Martin Leucker. 2010. Regular Linear Temporal Logic with Past. In *Verification, Model Checking, and Abstract Interpretation, 11th International Conference, VMCAI 2010, Madrid, Spain, January 17-19, 2010. Proceedings (Lecture Notes in Computer Science, Vol. 5944)*, Gilles Barthe and Manuel V. Hermenegildo (Eds.). Springer, 295–311. https://doi.org/10.1007/978-3-642-11319-2_22
- [3] Zenodo. 2023. Benchmark and Source Code. <https://zenodo.org/records/8388488>.

Received 2023-09-22; accepted 2024-01-23