Commit 3e474c2

millert committed on Nov 8, 2025

```
exec_mailer: Set group as well as uid when running the mailer

Also make a setuid(), setgid() or setgroups() failure fatal.

Found by the ZeroPath AI Security Engineer <https://zeropath.com>
```

main

1 parent 8487210 commit 3e474c2

5 files changed +24 -8 lines changed

Top

Filter files…

- include
  - sudo_eventlog.h
- lib/eventlog
  - eventlog.c
  - eventlog_conf.c
- plugins/sudoers
  - logging.c
  - policy.c

5 files changed +24 -8 lines changed

Search within code

include/sudo_eventlog.h

```
@@ -80,6 +80,7 @@ struct eventlog_config {
80  80      int syslog_rejectpri;
81  81      int syslog_alertpri;
```

```
82  82          uid_t mailuid;
    83  +       gid_t mailgid;
83  84          bool omit_hostname;
84  85          const char *logpath;
85  86          const char *time_fmt;
                @@ -151,7 +152,7 @@ void eventlog_set_syslog_rejectpri(int pri);
151 152     void eventlog_set_syslog_alertpri(int pri);
152 153     void eventlog_set_syslog_maxlen(size_t len);
153 154     void eventlog_set_file_maxlen(size_t len);
154     -   void eventlog_set_mailuid(uid_t uid);
    155 +   void eventlog_set_mailuser(uid_t uid, gid_t gid);
155 156     void eventlog_set_omit_hostname(bool omit_hostname);
156 157     void eventlog_set_logpath(const char *path);
157 158     void eventlog_set_time_fmt(const char *fmt);
```

lib/eventlog/eventlog.c

```
                @@ -299,15 +299,13 @@ exec_mailer(int pipein)
299 299         syslog(LOG_ERR, _("unable to dup stdin: %m")); // -V618
300 300         sudo_debug_printf(SUDO_DEBUG_ERROR,
301 301             "unable to dup stdin: %s", strerror(errno));
302     -       sudo_debug_exit(__func__, __FILE__, __LINE__, sudo_debug_subsys);
303     -       _exit(127);
    302 +       goto bad;
304 303         }
305 304
306 305         /* Build up an argv based on the mailer path and flags */
307 306         if ((mflags = strdup(evl_conf->mailerflags)) == NULL) {
308 307         syslog(LOG_ERR, _("unable to allocate memory")); // -V618
309     -       sudo_debug_exit(__func__, __FILE__, __LINE__, sudo_debug_subsys);
310     -       _exit(127);
    308 +       goto bad;
311 309         }
312 310         argv[0] = sudo_basename(mpath);
313 311
                @@ -326,11 +324,23 @@ exec_mailer(int pipein)
326 324         if (setuid(ROOT_UID) != 0) {
327 325         sudo_debug_printf(SUDO_DEBUG_ERROR, "unable to change uid to %u",
328 326             ROOT_UID);
```

```
      327 +     goto bad;
      328 +     }
      329 +     if (setgid(evl_conf->mailgid) != 0) {
      330 +     sudo_debug_printf(SUDO_DEBUG_ERROR, "unable to change gid to %u",
      331 +         (unsigned int)evl_conf->mailgid);
      332 +     goto bad;
      333 +     }
      334 +     if (setgroups(1, &evl_conf->mailgid) != 0) {
      335 +     sudo_debug_printf(SUDO_DEBUG_ERROR, "unable to set groups to %u",
      336 +         (unsigned int)evl_conf->mailgid);
      337 +     goto bad;
329   338       }
330   339       if (evl_conf->mailuid != ROOT_UID) {
331   340       if (setuid(evl_conf->mailuid) != 0) {
332   341           sudo_debug_printf(SUDO_DEBUG_ERROR, "unable to change uid to %u",
333   342           (unsigned int)evl_conf->mailuid);
      343 +         goto bad;
334   344       }
335   345       }
336   346       sudo_debug_exit(__func__, __FILE__, __LINE__, sudo_debug_subsys);
          @@ -342,6 +352,9 @@ exec_mailer(int pipein)
342   352       sudo_debug_printf(SUDO_DEBUG_ERROR, "unable to execute %s: %s",
343   353       mpath, strerror(errno));
344   354       _exit(127);
      355 + bad:
      356 +     sudo_debug_exit(__func__, __FILE__, __LINE__, sudo_debug_subsys);
      357 +     _exit(127);
345   358   }
346   359
347   360   /* Send a message to the mailto user */
```

lib/eventlog/eventlog_conf.c

```
          @@ -65,6 +65,7 @@ static struct eventlog_config evl_conf = {
65    65        LOG_ALERT,          /* syslog_rejectpri */
66    66        LOG_ALERT,          /* syslog_alertpri */
67    67        ROOT_UID,           /* mailuid */
      68 +     ROOT_GID,           /* mailgid */
68    69        false,          /* omit_hostname */
69    70        _PATH_SUDO_LOGFILE,     /* logpath */
```

```
70  71          "%h %e %T",          /* time_fmt */
    @@ -146,9 +147,10 @@ eventlog_set_file_maxlen(size_t len)
146 147     }
147 148
148 149     void
149     - eventlog_set_mailuid(uid_t uid)
    150 + eventlog_set_mailuser(uid_t uid, gid_t gid)
150 151     {
151 152         evl_conf.mailuid = uid;
    153 +     evl_conf.mailgid = gid;
152 154     }
153 155
154 156     void
```

plugins/sudoers/logging.c

```
    @@ -1152,7 +1152,7 @@ init_eventlog_config(void)
1152 1152         eventlog_set_syslog_alertpri(def_syslog_badpri);
1153 1153         eventlog_set_syslog_maxlen(def_syslog_maxlen);
1154 1154         eventlog_set_file_maxlen(def_loglinelen);
1155     -     eventlog_set_mailuid(ROOT_UID);
    1155 +     eventlog_set_mailuser(ROOT_UID, ROOT_GID);
1156 1156         eventlog_set_omit_hostname(!def_log_host);
1157 1157         eventlog_set_logpath(def_logfile);
1158 1158         eventlog_set_time_fmt(def_log_year ? "%h %e %T %Y" : "%h %e %T");
```

plugins/sudoers/policy.c

```
    @@ -634,7 +634,7 @@ sudoers_policy_deserialize_info(struct sudoers_context
    *ctx, void *v,
634 634         }
635 635
636 636     #ifdef NO_ROOT_MAILER
637     -     eventlog_set_mailuid(ctx->user.uid);
    637 +     eventlog_set_mailuser(ctx->user.uid, ctx->user.gid);
638 638     #endif
639 639
640 640         /* Dump settings and user info (XXX - plugin args) */
```

Comments 0

Please sign in to comment.