New issue

Jump to bottom

Usage-of-uninitialized value #1245

Closed xiaobaozidi opened this issue on Jun 29, 2021 · 3 comments · Fixed by #1246

Labels bug

xiaobaozidi commented on Jun 29, 2021 • edited Contributor

There are a few uninitialized value use bugs in src/mode/endpoints/mod_sofia/sofia.c

In function sofia_handle_sip_i_notify():
Array network_ip will be allocated in line 859

```
857                if (sofia_test_pflag(profile, PFLAG_FORWARD_MWI_NOTIFY)) {
858                        const char *mwi_status = NULL;
859                        char network_ip[80];
```

Then, it will be initialized by sofi_glue_get_addr()

867 sofia_glue_get_addr(de->data->e_msg, network_ip, sizeof(network_ip), NULL);
868 for (x = 0; x < profile->acl_count; x++) {
869 last_acl = profile->acl[x];
870 if (!(acl_ok = switch_check_network_list_ip(network_ip, last_acl))) {
871 break;

However, sofi_glue_get_addr() may return earlier, leading network_ip in an uninitliazed state.
Then network_ip will be used in switch_check_network_list_ip(). It may bypass (ACL) security checks due to the uninitialized value of network_ip, leading to privilege escalation.

Same in:

```
1618                if (authorization) {
1619                        char network_ip[80];
1620                        int network_port;
1621                        sofia_glue_get_addr(de->data->e_msg, network_ip, sizeof(network_ip), &network_port);
1622                        auth_res = sofia_reg_parse_auth(profile, authorization, sip, de,
1623                                                                                                (char *) sip->sip_request->rq_method_name, tech_pvt->key, strlen(tech_pvt->key),
network_ip, network_port, NULL, 0,
1624                                                                                                REG_INVITE, NULL, NULL, NULL, NULL);
1625                }
```

and in function sofia_handle_sip_i_reinvite()

```
10195                char network_ip[80];
10196                int network_port = 0;
10197                char via_space[2048];
10198                char branch[16] = "";
10199
10200                sofia_glue_store_session_id(session, profile, sip, 0);
10201
10202                sofia_clear_flag(tech_pvt, TFLAG_GOT_ACK);
10203
10204                sofia_glue_get_addr(de->data->e_msg, network_ip, sizeof(network_ip), &network_port);
10205                switch_stun_random_string(branch, sizeof(branch) - 1, "0123456789abcdef");
10206
10207                switch_snprintf(via_space, sizeof(via_space), "SIP/2.0/UDP %s;rport=%d;branch=%s", network_ip, network_port, branch);
```

and in function sofia_handle_sip_i_invite()

```
10311        char network_ip[80];
....

10394        sofia_glue_get_addr(de->data->e_msg, network_ip, sizeof(network_ip), &network_port);
10395
10396        switch_log_printf(SWITCH_CHANNEL_SESSION_LOG(tech_pvt->session), SWITCH_LOG_INFO, "%s receiving invite from %s:%d version: %s call-id: %s\n",
10397                                          switch_channel_get_name(tech_pvt->channel), network_ip, network_port, switch_version_full_human(), sip->sip_call_id ?
switch_str_nil(sip->sip_call_id->i_id) : "");
10398
```

sofi_glue_get_addr() may return earlier, leading network_ip in an uninitialized state. Then network_ip will be used in
function switch_log_printf(). This function may print out sensitive data that network_ip contained from previous stack.

Fix: set network_ip[80] = " ", preventing from uninitlized value use.

Thank you for the review, I also report this bug to CVE.

xiaobaozidi added the bug label on Jun 29, 2021

andywolk commented on Jun 29, 2021 — Contributor

@xiaobaozidi Can you make a PR? I will be happy to review it.

xiaobaozidi commented on Jun 29, 2021 — Contributor, Author

Sure


xiaobaozidi mentioned this issue on Jun 29, 2021

[mod_sofia] Fixed a few Usage-of-uninitialized value bugs which may cause information discolsure and bypass ACL check #1246

Merged


andywolk linked a pull request on Jul 24, 2021 that will close this issue

[mod_sofia] Fixed a few Usage-of-uninitialized value bugs which may cause information discolsure and bypass ACL check #1246 — Merged


andywolk closed this as completed in #1246 on Jul 24, 2021

---

andywolk commented on Jul 24, 2021 — Contributor

Thank you.

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

[mod_sofia] Fixed a few Usage-of-uninitialized value bugs which may cause information discolsure and bypass ACL check
xiaobaozidi/freeswitch

2 participants