

[New issue](#)[Jump to bottom](#)

isisd: misusing strdup leads to stack overflow #10505

Closed

whichbug opened this issue on Feb 5 · 6 comments · Fixed by #10566

Assignees



Labels

triage

whichbug commented on Feb 5 · edited

At Line 470 in the code below, we call `yang_data_new`, which will further call `strdup(raw_pdu)`. However, `raw_pdu` is not guaranteed to be a zero-terminated string and, thus, will lead to a stack overflow in `strdup`. When I set `raw_pdu[raw_pdu_len - 1]` to `\0`, then the bug disappears. Note that `strdup` should be used with a C-string.

In the same file, `isis_nb_notifications.c`, there are **8 places** where `yang_data_new` are used with `raw_pdu` and, thus, may have the overflow bug. Please check and suggest a fix. I can give a pull request then.

[frr/isisd/isis_nb_notifications.c](#)


Lines 454 to 471 in eef8006

```
454     void isis_notif_id_len_mismatch(const struct isis_circuit *circuit,
455                                     uint8_t rcv_id_len, const char *raw_pdu,
456                                     size_t raw_pdu_len)
457     {
458         const char *xpath = "/frr-isisd:id-len-mismatch";
459         struct list *arguments = yang_data_list_new();
460         char xpath_arg[XPATH_MAXLEN];
461         struct yang_data *data;
462         struct isis_area *area = circuit->area;
463
464         notif_prep_instance_hdr(xpath, area, "default", arguments);
465         notif_prepr_iface_hdr(xpath, circuit, arguments);
```

What follows is the output of the address sanitizer:

```
==48351==ERROR: AddressSanitizer: dynamic-stack-buffer-overflow on address 0x7ffe596a3a76 at pc
0x000000543e97 bp 0x7ffe596a3020 sp 0x7ffe596a27e0
```

```
READ of size 23 at 0x7ffe596a3a76 thread T0
#0 0x543e96 in strdup (/home/parallels/myfrr/isisd/isisd+0x543e96)
#1 0x84f73d in yang_data_new /home/parallels/myfrr/lib/yang.c:608:17
#2 0x6716eb in isis_notif_id_len_mismatch
/home/parallels/myfrr/isisd/isis_nb_notifications.c:470:9
#3 0x5cedcf in isis_handle_pdu /home/parallels/myfrr/isisd/isis_pdu.c:1706:3
```

 **whichbug** added the **triage** label on Feb 5

whichbug commented on Feb 8

Author

@idryzhov Could you also have a look at this issue?

 **donaldsharp** assigned **idryzhov** on Feb 8

idryzhov commented on Feb 9 • edited ▼

Contributor

Hi @whichbug, I checked the issue. The problem here is that we're trying to represent binary data as a simple string, which is wrong.

The only correct solution here would be to implement new function `yang_data_new_binary(const char *xpath, const char *binary, size_t len)` which will create a correct textual representation of YANG binary data, which is Base 64 Encoding. And then use this function instead of simple `yang_data_new` whenever we need to convert `raw_pdu`.

I probably won't find time to implement it in the next couple of days, so feel free to submit a PR.

whichbug commented on Feb 9

Author

Hi @whichbug, I checked the issue. The problem here is that we're trying to represent binary data as a simple string, which is wrong.

The only correct solution here would be to implement new function `yang_data_new_binary(const char *xpath, const char *binary, size_t len)` which will create a correct textual representation of YANG binary data, which is Base 64 Encoding. And then use this function instead of simple `yang_data_new` whenever we need to convert `raw_pdu`. I probably won't find time to implement it in the next couple of days, so feel free to submit a PR.

Hi, @idryzhov thanks for your reply. I think your idea makes sense and I will try.

qlyoung commented on Feb 10 • edited ▼

Member

Nice find. By the way, when you find issues like this, if you want you can just submit a pull request without filing an issue. We patch these kinds of things regularly without making an issue, since the pull request itself is records of both the issue and the appropriate fix for it. It's a little easier for us since we can track it in one place, and it helps keep our issues a little cleaner. It's up to you though.

 whichbug pushed a commit to whichbug/fr that referenced this issue on Feb 10

isisd: fix [FRRouting#10505](#) using base64 encoding ...

a7109ea

 whichbug pushed a commit to whichbug/fr that referenced this issue on Feb 10

isisd: fix [FRRouting#10505](#) using base64 encoding ...

2440ce7

  whichbug mentioned this issue on Feb 10

isisd: use base64 to encode the binary data. #10566

 Merged

 whichbug pushed a commit to whichbug/fr that referenced this issue on Feb 10

isisd: fix [FRRouting#10505](#) using base64 encoding ...

c35d739

whichbug commented on Feb 10

Author

Nice find. By the way, when you find issues like this, if you want you can just submit a pull request without filing an issue. We patch these kinds of things regularly without making an issue, since the pull request itself is records of both the issue and the appropriate fix for it. It's a little easier for us since we can track it in one place, and it helps keep our issues a little cleaner. It's up to you though.

Sure. Many thanks!

 whichbug pushed a commit to whichbug/fr that referenced this issue on Feb 11












isisd: fix [FRRouting#10505](#) using base64 encoding ...

3e7221d

 whichbug pushed a commit to whichbug/fr that referenced this issue on Feb 11

isisd: fix [FRRouting#10505](#) using base64 encoding ...

177e735

-  **whichbug** pushed a commit to whichbug/fr that referenced this issue on Feb 19
- isisd: fix [FRRouting#10505](#) using base64 encoding ... 8adc385
-  **whichbug** pushed a commit to whichbug/fr that referenced this issue on Feb 19
- isisd: fix [FRRouting#10505](#) using base64 encoding ... c683634
-  **whichbug** pushed a commit to whichbug/fr that referenced this issue on Feb 19
- isisd: fix [FRRouting#10505](#) using base64 encoding ... 075c3ac
-  **whichbug** pushed a commit to whichbug/fr that referenced this issue on Feb 19
- isisd: fix [FRRouting#10505](#) using base64 encoding ... b90ea44
-  **whichbug** pushed a commit to whichbug/fr that referenced this issue on Feb 19
- isisd: fix [FRRouting#10505](#) using base64 encoding ... 88b4165
-  **whichbug** pushed a commit to whichbug/fr that referenced this issue on Feb 19
- isisd: fix [FRRouting#10505](#) using base64 encoding ... de6945a
-  **whichbug** pushed a commit to whichbug/fr that referenced this issue on Feb 19
- isisd: fix [FRRouting#10505](#) using base64 encoding ... e5e412b
-  **whichbug** pushed a commit to whichbug/fr that referenced this issue on Feb 19
- isisd: fix [FRRouting#10505](#) using base64 encoding ... a48a73c
-  **whichbug** pushed a commit to whichbug/fr that referenced this issue on Feb 22
- isisd: fix [FRRouting#10505](#) using base64 encoding ... e3b45c6
-  **whichbug** pushed a commit to whichbug/fr that referenced this issue on Feb 22
- isisd: fix [FRRouting#10505](#) using base64 encoding ... 5493aee
-  **whichbug** pushed a commit to whichbug/fr that referenced this issue on Feb 22

isisd: fix [FRRouting#10505](#) using base64 encoding ...

285afc8

 **whichbug** pushed a commit to whichbug/frr that referenced this issue on Feb 22

isisd: fix [FRRouting#10505](#) using base64 encoding ...

4eb2b34

 **whichbug** pushed a commit to whichbug/frr that referenced this issue on Feb 22

isisd: fix [FRRouting#10505](#) using base64 encoding ...

a00d887


 **whichbug** pushed a commit to whichbug/frr that referenced this issue on Feb 22

isisd: fix [FRRouting#10505](#) using base64 encoding ...

ac31334

 **riw777** closed this as completed in [#10566](#) on Feb 28

 **plsaranya** pushed a commit to plsaranya/frr that referenced this issue on Feb 28

 isisd: fix [FRRouting#10505](#) using base64 encoding ...

ebec783

qlyoung commented on Mar 28 • edited ▼

Member

This is now filed as [CVE-2022-26126](#), with an assigned severity score of 7.8.


No assessment of exploitability has been made.

Please see my comment [here](#).

 **patrasar** pushed a commit to patrasar/frr that referenced this issue on Apr 28

 isisd: fix [FRRouting#10505](#) using base64 encoding ...


58e24d2

 **gpnavveen** pushed a commit to gpnavveen/frr that referenced this issue on Jun 7

isisd: fix [FRRouting#10505](#) using base64 encoding ...

59d0309

Assignees

 **idryzhov**

Labels

triage

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 isid: use base64 to encode the binary data.
whichbug/fr

3 participants

