Malá vítězství

Pavel Valach

CESNET

6. 6. 2024
Den IPv6 2024, Praha

Představení

Pavel Valach
člen bezpečnostního týmu CESNET-CERTS
součástí oddělení SOC

Představení

Pavel Valach
člen bezpečnostního týmu CESNET-CERTS
součástí oddělení SOC

a také:
divnočlověk, kterému občas něco začne tak vrtat v hlavě, že se toho nepustí, dokud nemá řešení nebo aspoň vysvětlení, hlavně když uvidí, že to už někdo udělal a přesto něco nejde z naprosto nelogických důvodů

Někdy je třeba do toho šťouchnout

if ipv6 ; then fail ; fi

And the IPv6 works when set manually, both SLAAC and DHCPv6.

TL;DR But the Huawei bearer in ModemManager does not support IPv6 at all.

Turns out that the error message is hardcoded in the bearer code for `huawei` plugin - src/plugins/huaw bearer-huawei.c on line 349.

```
349 if (ip_family != MM_BEARER_IP_FAMILY_IPV4) {
350     g_task_return_new_error (task,
351                              MM_CORE_ERROR,
352                              MM_CORE_ERROR_UNSUPPORTED,
353                              "Only IPv4 is supported by this modem");
354     g_object_unref (task);
355     return;
356 }
```

zdroj: https://gitlab.freedesktop.org/mobile-broadband/ModemManager/-/issues/87

Fix v ModemManageru

- Modem Huawei E3372 ve stick režimu (tj. bez webového NATu)
- IPv6 dostupná v některých firmwarech, či po povolení v NVRAM

- Vznikl Merge request (MR) do ModemManageru (nejsem autorem!)
- MR v ModemManageru vedl k opravě v NetworkManageru (jsem autorem)

- 2 MRs down, 1 to go :)
  - MR pro podporu IPv6 DNS přes signalizaci

Někdy to ostatní začnou řešit sami od sebe

Někdy to ostatní začnou řešit sami od sebe

- Naše maily ČVUTu padaly do spamu, tak se ozvali.

Někdy to ostatní začnou řešit sami od sebe

- Naše maily ČVUTu padaly do spamu, tak se ozvali.
- *Společný jmenovatel?*

Někdy to ostatní začnou řešit sami od sebe

- Naše maily ČVUTu padaly do spamu, tak se ozvali.
- *Společný jmenovatel?* **Odesláno po IPv6?!**

Někdy to ostatní začnou řešit sami od sebe

- Naše maily ČVUTu padaly do spamu, tak se ozvali.
- *Společný jmenovatel?* **Odesláno po IPv6?!**
- Přijímací server: MS Exchange či Office 365

V hlavičkách se objevilo toto:

```
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
cesnet.cz discourages use of 2001:718:1:a:b:c:d:e as permitted
sender)
```

SPF [RFC 7208]

Z metodiky NÚKIBu „k zavedení zvýšení ochrany e-mailové komunikace“:

- Technologie SPF (Sender Policy Framework) umožňuje organizaci definovat, které SMTP servery mohou posílat elektronické poštovní zprávy z domény organizace.
- Zobrazit existující SPF záznam pro doménu lze pomocí příkazu `dig` nebo `nslookup`. SPF záznam začíná hodnotou `v=spf1`.

zdroj: `https://nukib.gov.cz/download/uredni_deska/2021-10-08_Metodika_final.pdf`

Náš SPF záznam

```
$ dig txt cesnet.cz
```

Běžný SPF záznam:

```
v=spf1 ip4:147.32.110.2 a:lust.sin.cvut.cz ~all
```

Náš, méně obvyklý SPF záznam:

```
v=spf1 exists:%{ir}.spf.cesnet.cz include:servers.mcsv.net ~all
```

:(
Všechno nešlo hladce

- ČVUT otevřel lístek u podpory MS.
- *... chvíle napětí ...*

:(
Všechno nešlo hladce

- ČVUT otevřel lístek u podpory MS.
- *... chvíle napětí ...*

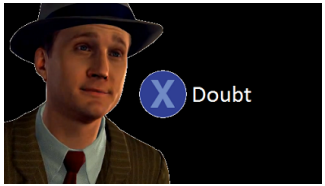
- Prý je chyba u nás.

Z e-mailu podpory MS: *Since the location is not specified in the SPF record, it is showing the Soft Fail. From the sender side SPF, the IPv6 has not been specified in the record.*

No a co je teda špatně?

```
Received-SPF: SoftFail (protection.outlook.com: domain of
transitioning cesnet.cz discourages use of 2001:718:1:a:b:c:d:e
as permitted sender)
```

Tj. IPv6 `2001:718:1:a:b:c:d:e` není oprávněná odesílat zprávy z naší domény `cesnet.cz`.



Náš SPF záznam

```
$ dig txt cesnet.cz
```

Běžný SPF záznam:

```
v=spf1 ip4:147.32.110.2 a:lust.sin.cvut.cz ~all
```

Náš, méně obvyklý SPF záznam:

```
v=spf1 exists:%{ir}.spf.cesnet.cz include:servers.mcsv.net ~all
```

exists:%{ir}.spf.cesnet.cz

- Jak funguje klíčové slovo `exists` v SPF záznamu?
  - Pokud existuje DNS záznam dle dané šablony, pak je adresa autorizována.
  - Makro `%{ir}` zpracuje IPv6 adresu serveru odesílajícího SMTP serveru – rozšíří na úplný tvar, rozloží do tečkované notace (*dot-format address*), a po vzoru DNS obrátí pořadí

`2001:718:1:a:b:c:d:e` → `2001:0718:0001:000a:000b:000c:000d:000e` →
`2.0.0.1.0.7.1.8.0.0.0.1.0.0.0.a.0.0.0.b.0.0.0.c.0.0.0.d.0.0.0.e` →
`e.0.0.0.d.0.0.0.c.0.0.0.b.0.0.0.a.0.0.0.1.0.0.0.8.1.7.0.1.0.0.2`

exists:%{ir}.spf.cesnet.cz

- Jak funguje klíčové slovo `exists` v SPF záznamu?
  - Pokud existuje DNS záznam dle dané šablony, pak je adresa autorizována.
  - Makro `%{ir}` zpracuje IPv6 adresu serveru odesílajícího SMTP serveru – rozšíří na úplný tvar, rozloží do tečkované notace (*dot-format address*), a po vzoru DNS obrátí pořadí

`2001:718:1:a:b:c:d:e` → `2001:0718:0001:000a:000b:000c:000d:000e` →
`2.0.0.1.0.7.1.8.0.0.0.1.0.0.0.a.0.0.0.b.0.0.0.c.0.0.0.d.0.0.0.e` →
`e.0.0.0.d.0.0.0.c.0.0.0.b.0.0.0.a.0.0.0.1.0.0.0.8.1.7.0.1.0.0.2`

DNS dotaz na příslušný `A` záznam pak vrátí `127.0.0.2` → **IP autorizována.**

```
e.0.0.0.d.0.0.0.c.0.0.0.b.0.0.0.a.0.0.0.1.0.0.0.8.1.7.0.1.0.0.2
        .spf.cesnet.cz. 3600 IN A 127.0.0.2
```

Makro %{ir}.spf.cesnet.cz

```
; mailer A
a.0.0.0.d.0.0.0.c.0.0.0.b.0.0.0.a.0.0.0.1.0.0.0.8.1.7.0.1.0.0.2
      .spf.cesnet.cz. 3600 IN A 127.0.0.2
```

Mailer A – 2001:718:1:A:B:C:D:A – může odesílat zprávy.

Makro %{ir}.spf.cesnet.cz

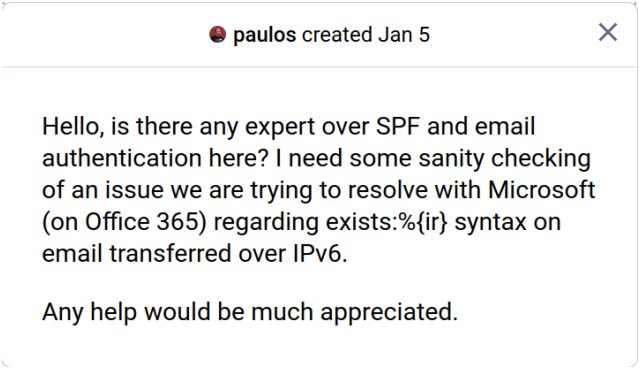
```
; mailer A
a.0.0.0.d.0.0.0.c.0.0.0.b.0.0.0.a.0.0.0.1.0.0.0.8.1.7.0.1.0.0.2
      .spf.cesnet.cz. 3600 IN A 127.0.0.2
```

Mailer A – 2001:718:1:A:B:C:D:A – může odesílat zprávy.

```
; mailer F
+ f.0.0.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.1.0.0.0.8.1.7.0.1.0.0.2
      .spf.cesnet.cz. 3600 IN A 127.0.0.2
```

Mailer F – 2001:718:1:1:2:3:4:F – může nyní také odesílat zprávy.

Zkouším sílu ~~Twitteru~~ Mastodonu



zdroj: `https://infosec.exchange/@paulos/111703214699173134`

Zkouším sílu ~~Twitteru~~ Mastodonu

Potvrdilo se, že:

- naše implementace je korektní,
- kontroly SPF v O365 / Exchange Online se chovají jinak (nekonformně s RFC 7208),
- *přesvědčit o tom MS bude trvat.*

Příčina – Co dělá O365?

Příčina – Co dělá O365?

Místo dotazu na

```
e.0.0.0.d.0.0.0.c.0.0.0.b.0.0.0.a.0.0.0.1.0.0.0.8.1.7.0.1.0.0.2
.spf.cesnet.cz.
```

proběhne dotaz na

Příčina – Co dělá O365?

Místo dotazu na

```
e.0.0.0.d.0.0.0.c.0.0.0.b.0.0.0.a.0.0.0.1.0.0.0.8.1.7.0.1.0.0.2
.spf.cesnet.cz.
```

proběhne dotaz na

`e.0.d.0.c.0.b.0.a.0.1.0.18.7.1.20.spf.cesnet.cz.`

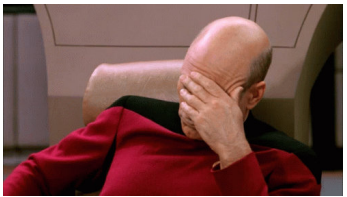
Příčina – Co dělá O365?

Místo dotazu na

```
e.0.0.0.d.0.0.0.c.0.0.0.b.0.0.0.a.0.0.0.1.0.0.0.8.1.7.0.1.0.0.2
.spf.cesnet.cz.
```

proběhne dotaz na

e.0.d.0.c.0.b.0.a.0.1.0.18.7.1.20.spf.cesnet.cz.



Místo po nibblech
tečkují vždy po celých bytech!

Cesta k srdci MS

1. Podívat se, co píše RFC 7208

RFC 7208

Sekce 7.3. Macro Processing Details:

...
For IPv6 addresses, the "i" macro expands to a dot-format address; it is intended for use in %{ir}. ...

Sekce 7.4. Expansion Examples:

```
IPv6:
%{ir}.%{v}._spf.%{d2}                                    1.0.b.c.0.0.0.0.
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6._spf.example.com
```

zdroj: `https://datatracker.ietf.org/doc/html/rfc7208#section-7.3`

Cesta k srdci MS

1. Podívat se, co píše RFC 7208
2. Reprodukce problému na vlastní infrastruktuře

Vlastní testy

Nastavení SPF záznamu pro doménu `omg.paulos.cz`:

```
v=spf1 exists:%{ir}.spf.omg.paulos.cz ~all
```

IPv6 e-mail z mojí adresy `(na) omg.paulos.cz` → `(na) cvut.cz` vygeneroval od MS následující DNS dotaz:

```
AQ 13.74.17.204:52376 -> 0.0.0.0:53 UDP 72b 1.0.0.0.0.0.0.0.cd.1.fe.0.40.3b.3.2a.spf.omg.paulos.cz/IN/A
AQ 13.105.166.85:25341 -> 0.0.0.0:53 UDP 42b OMG.PAULOS.CZ/IN/A
AR 13.74.17.204:52376 <- 0.0.0.0:53 UDP 126b 1.0.0.0.0.0.0.0.cd.1.fe.0.40.3b.3.2a.spf.omg.paulos.cz/IN/A
```

Po nastavení DNS záznamu pro `1.0.0.0.0.0.0.0.cd.1.fe.0.40.3b.3.2a.spf.omg.paulos.cz` SPF ověření prošlo.

Cesta k srdci MS

1. Podívat se, co píše RFC 7208
2. Reprodukce problému na vlastní infrastruktuře
3. Nahlášení znovu, eskalace
   - Podrobné popsání, kdy k problému dochází a jaké podmínky musí být splněny, aby k problému došlo – vzácný případ
   - Nemilosrdná eskalace, že jde o nesoulad s RFC

Cesta k srdci MS

1. Podívat se, co píše RFC 7208
2. Reprodukce problému na vlastní infrastruktuře
3. Nahlášení znovu, eskalace
   - Podrobné popsání, kdy k problému dochází a jaké podmínky musí být splněny, aby k problému došlo – vzácný případ
   - Nemilosrdná eskalace, že jde o nesoulad s RFC

Druhé nahlášení problému MS v lednu 2024.
Microsoft problém začal řešit na konci ledna 2024 – tj. po dvou, třech týdnech.
Urgence na začátku dubna – zatím neopraveno – ale uznali bug.
Stav k 6. 6. 2024 – oprava zatím nebyla nasazena.

Poděkování

- kolegům z CESNETu
- VIC ČVUT
- Patrick "Jima" Laughton, Colin Cogle

Poděkování

Děkuji Vám za pozornost.

Dotazy?

Teď, nebo ~~nikdy~~ později na pavel.valach@cesnet.cz