権威DNSサーバを作ってみよう

ゼロから始めるファジング生活 updated

JANOG 42.5 Interim Meeting
2018/10/19

坂口俊文

自己紹介

坂口　俊文

- 5年前までは、ISPのメール・DNS…サーバの管理者
- 現在はとあるクラウドサービスのサポート
- Twitter: @siskrn
- GitHub: https://github.com/sischkg/
- DNS Summer Day, DNSOPS.JP BoFで発表 https://dnsops.jp/
- 主な実績
  - PowerDNS Advisory 2015-1
  - CVE-2016-2848(A packet with malformed options can trigger an assertion failure in ISC BIND versions released prior to May 2013 and in packages derived from releases prior to that date)

はじめに

本日は、最近開発・利用しているDNSフルリゾルバ専用のファジングツールについて発表します。

今年のDNS Summer Dayの発表の概要+Updateとなります。

- ワイルドカード対応
- 毒入れ(Cache Poisoning)チェック
- Knot Resolver 2.4.0において修正された不具合の件

ファジングとは

- バグや未知の脆弱性を検出するセキュリティテスト
- 問題が起きそうな様々な細工をしたデータを送り、検査対象に異常な動作が起きないかどうかを検査
- 問題を起こしそうなデータは、ファジングツールを使うと自動的に作成することができる

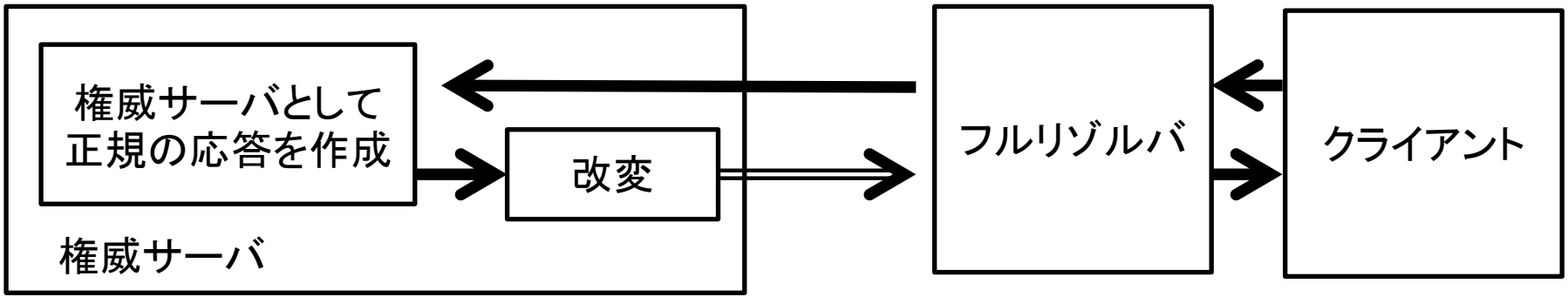
詳細

IPA : 情報セキュリティ :ファジング：FAQ

https://www.ipa.go.jp/security/vuln/fuzz_faq.html#001

ファジングツールの概要

- 最初に権威サーバとして正規の応答を作成し、それを改変してからフルリゾルバへ送信する
- 特殊な応答は乱数をもとに作成
- フルリゾルバが異常終了（assertion failure/segmentation fault)する不具合を探す
- 毒入れもチェック



権威サーバの実装

- DNSSECに対応（RRSetの署名/NSEC/NSEC3)
- 完全な権威サーバを実装しない
  - ゾーンはひとつのみ
  - 以下の機能は未実装
    - ~~ワイルドカード~~　実装済み
    - NSEC3 Opt-out
    - TSIG

    など

ファジングの実装

過去の(BINDなどの)脆弱性を参考に実装

- RRの追加
  - 乱数からCLASS, TYPE, TTL, RDATAを自動生成
- RRの変更
  - RRのクラスを変更（IN → CH/HS/ANY/NONE)
- RRの削除
- OPT RR
  - 乱数からPAYLOAD SIZE/OPTIONを自動生成
- RCODEの変更
- 署名(DNSSEC)
- 各セクションでのRRの順序変更
- DNSメッセージの変更
  - バイナリデータの追加・変更・削除

ファジングの実装

クライアント（スタブリゾルバ）

- クエリの作成
  - QNAMEを権威サーバ側のゾーンデータをもとに生成
  - 乱数からQTYPE, QCLASSを生成
  - OPTのバージョン、ペイロードサイズ、OPTIONを乱数から生成
- クエリを一定間隔でフルリゾルバへ送信

ファジングの実装

- 動作確認
  - Zabbix(Simple check)によるフルリゾルバのサービス確認
  - digによる目視チェック

- 原因調査
  - パケットキャプチャ
  - ログ（assertion failure/segentation fault)
  - CORE解析

例1

```
$ dig @127.0.0.1 www.example.com a +dnssec +norec
;; Warning: Message parser reports malformed message packet.

; <<>> DiG 9.9.4-RedHat-9.9.4-51.el7_4.2 <<>> @127.0.0.1 www.example.com a +dnssec +norec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42115
;; flags: qr aa ad; QUERY: 1, ANSWER: 5, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: Message has 3319 extra bytes at end

;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        10      IN      A       192.168.0.101
www.example.com.        10      IN      A       192.168.0.102
www.example.com.        961138880 HS    DNAME   \028\159fc\167,\191\2005\181p\186KG\198m\209\226\014\200\236\152\21
5I\209\030\018\133\169\192\152\197`\000*\135\171i\207`\159\192\027\234.\251\158\174\135\014\180\015}knk\152\209\173
\183\235{\196e_\144\240S\199\008\196\\\161\137v\167\005\021V\012\162\138\027\159\245\138\138\015\\9\198\2004\012.\1
50>\018\144\236\139|\220\131\211\133\2357\005\)\012n\133\008\2397\223\237-c\194\159\154\204\013y\227K\139t\183\150q
\020\153\196.\031\167\151\212\219|\197\171W\2513\180{\168\012P\178z\173ylp\246V\168\232\227\000=\212i\\|\001\176\21
5\253v\003U\2417\138.www.example.com.
www.example.com.        10      IN      RRSIG   A 13 3 10 20180613124222 20180603124222 59425 example.com. 3aJpbgbW
8Xf2tIBdMi3MvjKVc8NCmxwNxFk+qhab9yV3/AQcDMO+pVIJ Mpa9Ivt78N4aCzXD0cNvvAx0u6WGsw==
www.example.com.        961138880 HS    RRSIG   DNAME 13 3 961138880 20180613124222 20180603124222 59425 example.co
m. 3CvHapBLSvYyeFGSbeQkBaq6oWXbKIN2vEGZGnlBshJjIeP2uIdClQNB qdYEPghafzJFCwOAEBwIxJFJjnT+yQ==
```

例2

```
$ dig @127.0.0.1 www.example.com a +dnssec +norec
;; Warning: Message parser reports malformed message packet.
;; Truncated, retrying in TCP mode.
;; Got bad packet: bad compression pointer
8746 bytes
32 fb 84 20 00 01 00 03 00 04 00 01 03 77 77 77          2............www
07 65 78 61 6d 70 6c 65 03 63 6f 6d 00 00 01 00          .example.com....
01 c0 0c 00 01 00 01 00 00 00 0a 00 04 c0 a8 00          ................
65 c0 0c 00 01 00 01 00 00 00 0a 00 04 c0 a8 00          e...............
66 c0 0c 00 2e 00 01 00 00 00 0a 00 5f 00 01 0d          f..........._...
03 00 00 00 0a 5b 21 11 2e 5b 13 e2 2e e8 21 07          .....[!..[....!.
65 78 61 6d 70 6c 65 03 63 6f 6d 00 a8 60 6c 7f          example.com..`l.
5f 7c d7 4a a7 5c 83 f4 ee d9 62 29 71 42 1d ce          _|.J.\....b)qB..
46 89 8a c6 c0 b7 4a f3 0f 9c 86 91 0f 91 31 5d          F.....J.......1]
65 1a 64 96 55 fe 54 c1 25 4f 3c d6 f3 02 3a f6          e.d.U.T.%O<...:.
08 df d6 25 37 ed c6 23 26 48 cf 19 c0 0c 00 2b          ...%7..#&H.....+
00 04 6c 1f 77 ed 00 24 0b 69 05 02 81 31 31 c1          ..l.w..$.i...11.
7b 47 e8 96 8a c1 2c b5 17 ce 0f 20 df be 26 47          {G....,.......&G
0c 2d b5 64 ee 45 2f 6a 03 43 99 84 c0 0c 00 0b          .-.d.E/j.C......
00 fe 44 97 5d 51 00 04 7b f5 aa 0f f4 5d 64 e4          ..D.]Q..{....]d.
64 8c 13 01 c4 5f 5b d7 40 85 35 00 9d 60 83 ad          d...._[.@.5..`..
0f 10 72 24 24 82 63 f3 45 bf 34 98 c6 e7 1f 42          ..r$$.c.E.4....B
c4 62 02 03 09 22 63 02 2c 19 44 22 40 92 26 b6          .b..."c.,.D"@.&.
e1 30 02 c3 62 e0 d7 78 cf 2f a2 28 30 aa 57 44          .0..b..x./.(0.WD
ae 84 bc 69 3b be d3 21 b3 65 70 c2 96 22 04 80          ...i;..!.ep.."..
40 4c ef 8c 81 c8 e0 86 48 f4 20 2b 3b 02 05 c0          @L......H..+;...
```

調査対象

- フルリゾルバ
  - BIND 9.12.x, 9.7.x(CentOS 6.x RPM)
  - Unbound
  - PowerDNS Recursor 4.1.x
  - Knot Resolver
- ついでに
  - dnsmasq
  - dnsdist
  - coredns

結果

- PowerDNS Security Advisory 2017-08: Crafted CNAME answer can cause a denial of service
  - https://doc.powerdns.com/recursor/security-advisories/powerdns-advisory-2017-08.html
- Knot Resolver: fix CVE-2018-1110: denial of service triggered by malformed DNS messages (2件の問題)

  https://lists.nic.cz/pipermail/knot-resolver-announce/2018/000000.html
  - https://gitlab.labs.nic.cz/knot/knot-resolver/issues/334
  - https://gitlab.labs.nic.cz/knot/knot-resolver/issues/335
- Knot-Resolver 2.3.0 crashes in module/stats.

  libknot(knot-dns 2.6.7未満)の"knot_dname_to_str memory overflow"に起因
  - https://gitlab.labs.nic.cz/knot/knot-dns/raw/v2.6.7/NEWS
  - https://gitlab.labs.nic.cz/knot/knot-resolver/issues/354

結果

- knot-resolver 2.3.0 aborted with "kresd: libknot/packet/pkt.c:84: pkt_wire_alloc: Assertion `len >= KNOT_WIRE_HEADER_SIZE' failed."
  - https://gitlab.labs.nic.cz/knot/knot-resolver/issues/366
  - DNSSEC Validation有効時に発生
  - 反復問い合わせ中のある状態で、DNSヘッダサイズより小さな応答を受信すると、強制終了する
  - 2.4.0で修正
  - ChangeLogでは"minimal libknot version is now 2.6.7 to pull in latest fixes (#366 (closed))"という扱い
    - 前スライドの"knot_dname_to_str memory overflow"対策に含まれる