ファジングツールのまとめ

DNS Summer Day 2019
2019/06/28
Toshifumi Sakaguchi

自己紹介

- 坂口　俊文
- Twitter: @siskrn
- GitHub: https://github.com/sischkg/
- DNS Summer Day, DNSOPS.JP BoFで発表 https://dnsops.jp/
- 主な実績
  - CVE-2015-1868(PowerDNS)
  - CVE-2016-2848(BIND)
  - CVE-2017-15120(PowerDNS)
  - CVE-2018-1110(Knot Resolver)
  - CVE-2018-14644(PowerDNS)
  - CVE-2018-5744(BIND)

Agenda

- ファジングツールを開発した目的
- 復習
  - ファジングツールの概要
  - 昨年のDNS Summer Dayまでに公開された問題
- 新規に公開された問題
  - Knot Resolver 2.4.0において修正された不具合の件
  - CVE-2018-14644(PowerDNS Security Advisory 2018-07)
  - CVE-2018-5744(BINDメモリリーク)
- まとめ

ファジングツールを開発した目的

- ネットワークなどのプログラミングの習得
- DNSプロトコルの理解
- LTのネタ

ファジングツールを開発した目的(裏)

- うさぎさんにはまけないぞ

  American fuzzy lop (http://lcamtuf.coredump.cx/afl/)

- おこづかい

  HackerOneのPowerDNS Bug Bounty Program (https://hackerone.com/powerdns)

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

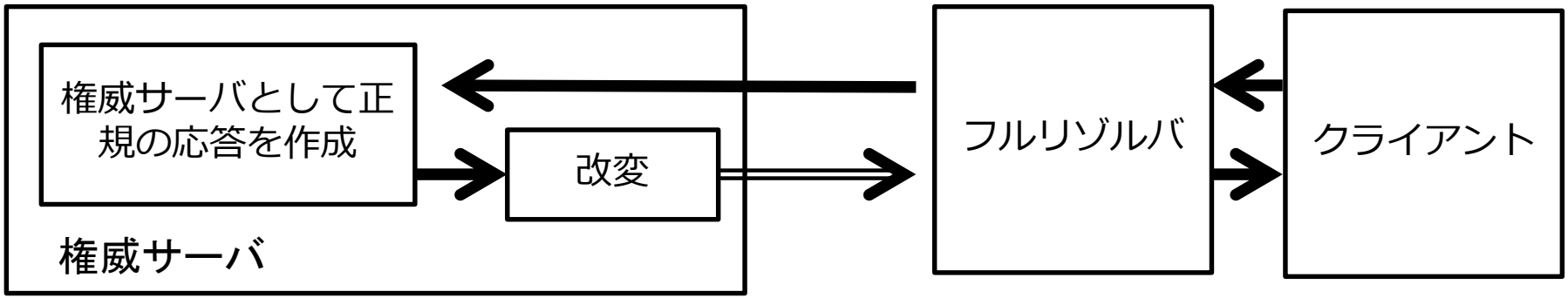
詳細

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
- フルリゾルバが異常終了（assertion failure/segmentation fault)する不具合を探す



調査対象

- BIND 9.7.x, 9.9.x, 9.11.x, 9.12.x, 9.14.x
- Unbound
- PowerDNS Recursor 3.x, 4.x
- Knot Resolver
- dnsdist
- dnsmasq
- coredns

昨年のDNS Summer Dayまでに公開された問題

- 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

DNS Summer Day 2018以降に公開された問題

Knot Resolverが異常終了する問題

- https://gitlab.labs.nic.cz/knot/knot-resolver/issues/366
- knot-resolver 2.3.0 aborted with "kresd: libknot/packet/pkt.c:84: pkt_wire_alloc: Assertion `len >= KNOT_WIRE_HEADER_SIZE' failed."
- Knot Resolver 2.3.0 以下が対象
- 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

PowerDNS Security Advisory 2018-07 (1)

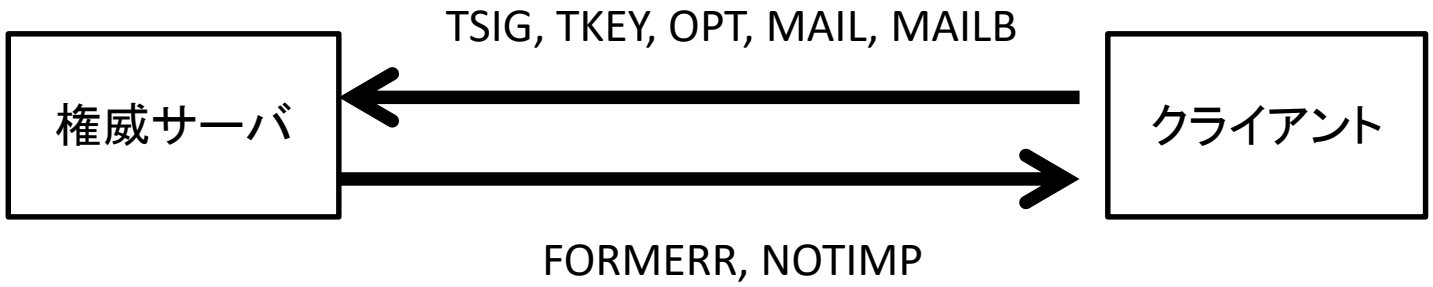
- Crafted query for meta-types can cause a denial of service
- https://doc.powerdns.com/recursor/security-advisories/powerdns-advisory-2018-07.html
- 対象: PowerDNS Recursor 4.0.0 – 4.0.8, 4.1.0 – 4.1.4
- DNSSEC Validation有効時に発生(dnssec=validate)
- 特定の条件を満たすゾーンとその子の名前解決に失敗する(BOGUS扱い)

PowerDNS Security Advisory 2018-07 (2)

条件

- 署名ゾーン
- ゾーンの権威サーバが以下の動作をする

  QTYPEがMETA RRもしくはDeprecatedの問い合わせに対して、RCODEがFORMERRもしくはNOTIMPを応答



PowerDNS Security Advisory 2018-07 (3)

QTYPE=Meta, Deprecated Typeの問い合わせに対する権威サーバの応答

QTYPE	BIND 9.11.4-P2	NSD 4.1.25	PowerDNS 4.1.4	Knot DNS 2.7.2
TSIG	***FORMERR***	NODATA	NODATA	NODATA
TKEY	***FORMERR***	NODATA	***FORMERR***	NODATA
OPT	***FORMERR***	NODATA	NODATA	NODATA
MAILA	***NOTIMP***	NODATA	NODATA	NODATA
MAILB	***NOTIMP***	NODATA	NODATA	NODATA

PowerDNS Security Advisory 2018-07 (4)

この条件を満たすゾーンの例

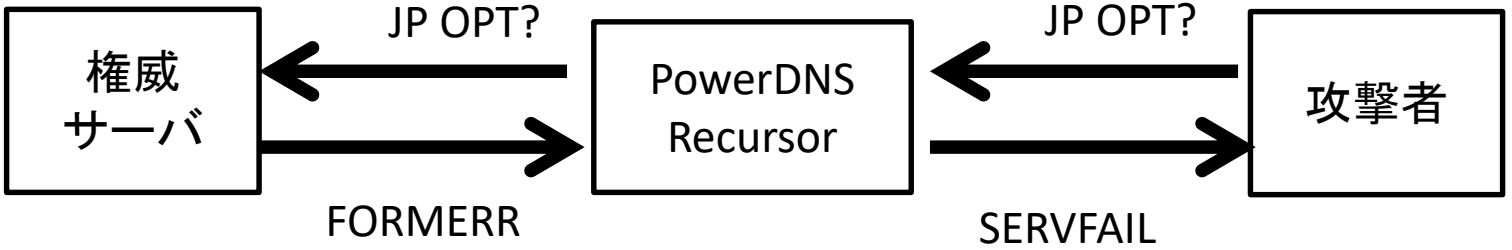
- .JP
- .COM
- .FR

PowerDNS Security Advisory 2018-07 (5)

1. ターゲットのPowerDNS Recursorに対して問い合わせを送信

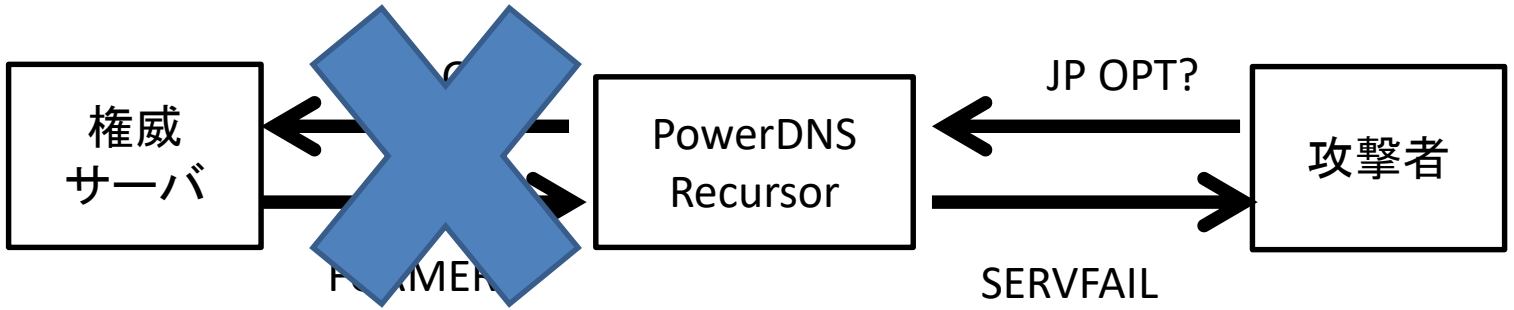
```
$ dig @target.example.com  JP  OPT
```

2. ターゲットはJPの権威サーバへクエリを送信しFORMERRを受信
3. 以後ターゲットはJPドメインの名前解決に失敗
   - JPの権威サーバをEND0未対応サーバと判断？
   - 一日継続



PowerDNS Security Advisory 2018-07 (6)

- 対策
  - PowerDNS Recursor 4.0.9, 4.1.5へバージョンアップ
    - Meta, Deprecated Typeの場合、権威サーバへ問い合わせない
- 回避策
  - DNSSEC検証しない



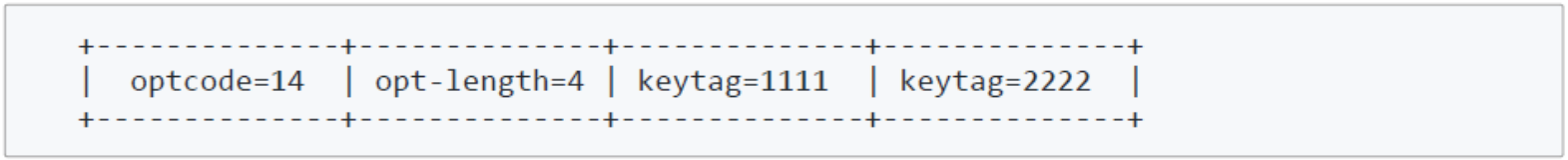
BINDメモリリーク

- A specially crafted packet can cause named to leak memory
- https://kb.isc.org/docs/cve-2018-5744
- 複数の Key Tag Option を持つDNSクエリを受信するとメモリリーク
- 対象
  - 9.10.7 - 9.10.8-P1
  - 9.11.3 - 9.11.5-P1
  - 9.12.0 - 9.12.3-P1

BINDメモリリーク (2)

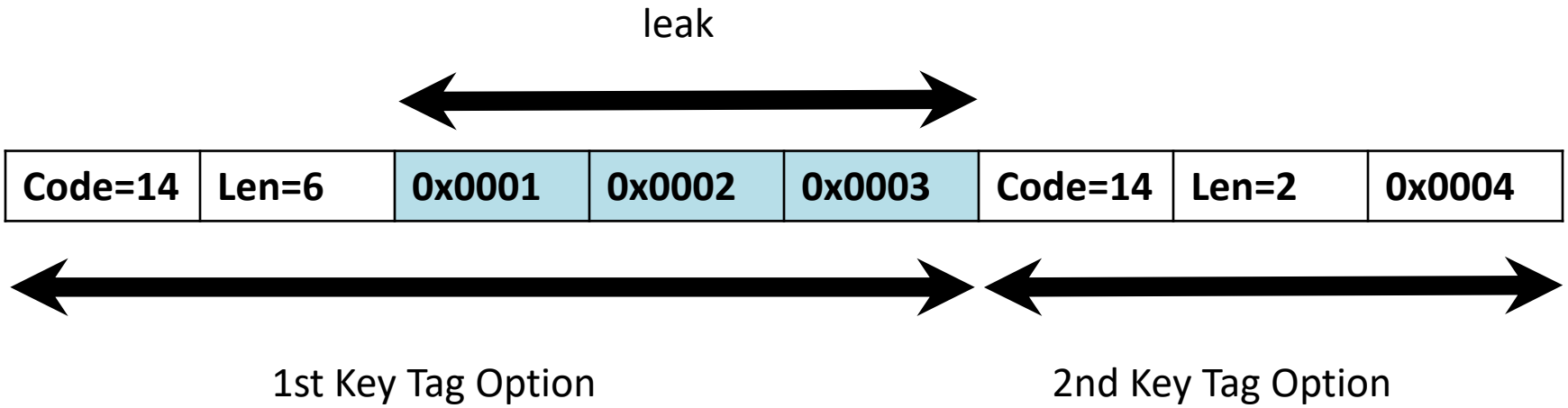
Key Tag Option

- RFC8145 Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)(https://tools.ietf.org/html/rfc8145)
  - Root KSK Rolloverのため
  - 新しいTrust AnchorをValidatorへ設定したかを調査するために導入
- Validatorが使用しているTrust AnchorのKey Tagを、EDNS0のオプションで権威サーバへ通知



BINDメモリリーク (3)

- ひとつのメッセージの中にN個のKey Tag Optionがある場合、1～N-1番目のKey Tag分のメモリがリーク
- 効率よくリークさせるには、最初のKey Tag Optionに多くのKey Tagを追加



BINDメモリリーク (4)

- Key Tag Optionを処理中に、Key Tag用のメモリを割り当て済みかをチェックしないため、メモリリークが発生

```
2110  static isc_result_t
2111  process_keytag(ns_client_t *client, isc_buffer_t *buf, size_t optlen) {
2112
2113          if (optlen == 0 || (optlen % 2) != 0) {
2114                  isc_buffer_forward(buf, (unsigned int)optlen);
2115                  return (DNS_R_OPTERR);
2116          }
2117
2118          client->keytag = isc_mem_get(client->mctx, optlen);
2119          if (client->keytag != NULL) {
2120                  client->keytag_len = (uint16_t)optlen;
2121                  memmove(client->keytag, isc_buffer_current(buf), optlen);
2122          }
2123          isc_buffer_forward(buf, (unsigned int)optlen);
2124          return (ISC_R_SUCCESS);
2125  }
2126
```

https://gitlab.isc.org/isc-projects/bind9/blob/v9_11_5_P1/bin/named/client.c#L2110

BINDメモリリーク(5)

対策

- バージョンアップ
  - 9.11.5-P4
  - 9.12.3-P4

回避策

- なし

まとめ

- Socket/Threadなどを利用したプログラムに一歩踏み込むことができた
- DNSSECなどDNSの理解は、まだこれから。
- 以下のLTにて発表
  1. DNS Summer Day 2018
  2. JANOG Interim 42.5
  3. DNS温泉番外編(2019/02/14)
  4. #ssmjp～DNSの話を聞く会～
  5. JANOG Interim 43.5(懇談会内)

まとめ

- フルリゾルバのみの限られたなかでCVE4件
  1. CVE-2017-15120(PowerDNS)
  2. CVE-2018-1110(Knot Resolver)
  3. CVE-2018-14644(PowerDNS)
  4. CVE-2018-5744(BIND)
- PowerDNS Bug BountyにてReward x 3

  ありがとうございました > PowerDNS