DNSメッセージの仕様による性能問題とその対策とこれから

2024年11月26日

Internet Week 2024 DNSOPS.JP BoF

坂口　俊文

自己紹介

- 坂口俊文
  - 所属: なし
  - X: @siskrn
  - 実績
    - CVE-2015-1868(PowerDNS Recursor)
    - CVE-2016-2848(BIND)
    - CVE-2017-15120(PowerDNS Recursor)
    - CVE-2018-1110(Knot Resolver)
    - CVE-2018-14644(PowerDNS Recursor)
    - CVE-2018-5744(BIND)
    - CVE-2024-1737(BIND) ⇐ New
    - CVE-2024-8508(Unbound) ⇐ New
    - CVE-2024-25590(PowerDNS Recursor) ⇐New

2024年に発見した性能問題

- BIND: CVE-2024-1737 BIND's database will be slow if a very large number of RRs exist at the same name
- Unbound: CVE-2024-8508 Unbounded name compression could lead to Denial of Service
- PowerDNS Recursor: CVE-2024-25590: Crafted responses can lead to a denial of service due to cache inefficiencies in the Recursor
- Knot Resolver: 脆弱性として扱われていないが、CPU使用率が上昇し応答が遅延する問題があり、libknot(knot DNS)が修正。

検証環境

- CPU: RYZEN 7 1700
- Memory 64GB
- Windows 10 ProにインストールしたVMware Workstation上の仮想マシン
  - Rocky Linux 9
  - 16 vCPU
  - 16 GBメモリ

BINDの性能問題

- CVE: CVE-2024-1737
- 概要: 同じドメイン名に大量のRRが設定されたデータをキャッシュしているフルリゾルバにおいて、クライアントからのクエリを処理したとき、namedのCPU使用率が増加し、応答の遅延やタイムアウトが発生。
- 対策: RRsetのレコード数の上限をmax-records-per-type(default: 100)に制限。同一ドメイン名のレコードのタイプ数の上限をmax-types-per-name(default: 100)に制限

BINDの性能問題

権威サーバに次のRRset(レコード数2000)を設定。

```
a.example.com.    IN A 192.0.2.1
a.example.com.    IN A 192.0.2.2
a.example.com.    IN A 192.0.2.3
…
```

フルリゾルバへこのRRsetのクエリを100qpsで送信。

```
$ echo “a.example.com A” > query_data.txt
$ resperf -d query_data.txt -c 1000 -m 100 -C 30 -R
```

Unboundの性能問題

- CVE: CVE-2024-8508
- 概要: 多くのラベルを含むドメイン名を持つ、非常に大きなRRsetをキャッシュしている場合、クライアントからのクエリを処理したとき、名前圧縮処理によりunboundのCPU使用率が増加し、応答の遅延やタイムアウトが発生。
- 対策: DNSメッセージ内での名前圧縮の回数を120に制限。

Unboundの性能問題

権威サーバに次のRRset(レコード数2000)を設定。各ドメイン名のラベル”0”はそれぞれ110個。

```
0.<snip>.0.example.com.  IN MX 10 mx1.0.<snip>.0.example.com.
0.<snip>.0.example.com.  IN MX 10 mx2.0.<snip>.0.example.com.
…
```

フルリゾルバへこのRRsetのクエリを1000qpsで送信。

- TransportはTCP
- 各クエリはフルリゾルバへDNSメッセージを送信後、リプライを待たずに接続を切断します。不要なトラフィックを避けるため。

PowerDNS Recursorの性能問題

- CVE: CVE-2024-25590
- 概要:多くのラベルを含むドメイン名を持つ、非常に大きなRRsetをキャッシュしているフルリゾルバにおいて、クライアントからのクエリを処理したとき、pdns-recursorのCPU使用率が増加し、応答の遅延やタイムアウトが発生。
- 対策: RRsetのレコード数の上限をmax-RRset-size(default: 256)に制限。

PowerDNS Recursorの性能問題

ゾーンexample.com.の権威サーバに次のレコードを設定。

```
*.example.com.  IN CNAME a.0.<snip>.0.example.com.
```

ゾーンexample.jp.の権威サーバに、次のRRset(レコード数2000)を設定。各ドメイン名のラベル”0”はそれぞれ110個。

```
a.0.<snip>.0.example.com.  IN A 192.0.2.1
a.0.<snip>.0.example.com.  IN A 192.0.2.2
…
```

フルリゾルバへ*.example.com (ランダムサブドメイン)のクエリを1000qpsで送信。

```
$ resperf -d random_query_data.txt -m 1000 -C 30
```

Knot Resolverの性能問題

- CVE: なし
- 概要: 非常に大きなRRsetをキャッシュしているフルリゾルバにおいて、クライアントからのクエリを処理したとき、kresdのCPU使用率が増加し応答の遅延が発生。
- 対策: ライブラリlibknot(Knot DNS)のパフォーマンスの改善。

Version 3.3.9
Monday, August 26, 2024

Improvements:

- libknot: added EDE code 30
- **libknot: improved performance of knot_RRset_to_wire_extra()**
- libs: upgraded embedded libngtcp2 to 1.7.0
- doc: various fixes and updates

Knot Resolverの性能問題

権威サーバに次のRRset(レコード数4000)を設定。

```
a.example.com.    IN A 192.0.2.1
a.example.com.    IN A 192.0.2.2
a.example.com.    IN A 192.0.2.3
…
```

フルリゾルバへこのRRsetのクエリを2000qpsで送信。

- TransportはTCP
- 各クエリはフルリゾルバへDNSメッセージを送信後、リプライを待たずに接続を切断します。不要なトラフィックを避けるため。

性能問題の比較

表の上のほうが攻撃が容易(QPSが少ない、UDPが利用可能)。

	攻撃側の用意するRRsetの特徴	Transport
BIND	RRsetのレコード数	UDP/TCP
PowerDNS Recusor	RRsetのレコード数とラベル数	UDP/TCP
Unbound	RRsetのレコード数とラベル数	TCP
Knot Resolver	RRsetのレコード数	TCP

DNSメッセージ内のレコード数

これらの問題はDNSメッセージ内に多数のレコードを入れることができることに起因する。

- DNSメッセージでは、ANCOUNT/NSCOUNT/ARCOUNTでレコード数を表しますが、符号なし16bit整数のため、実質的な上限値にはならない。
- レコード数の上限を決定するのは、DNSメッセージのサイズ上限。
  - TCP利用時の2^16-1(65,535)byte
- 名前圧縮により非常に多くのレコード(4000以上)を、ひとつのメッセージ内に入れることが可能。

NXNSAttackもこの性質を利用。

- このときに本問題を発見すべきだったかもしれない。

これからの課題

一部のフルリゾルバにおいて、RRsetのレコード数の上限値が導入

- メーリングリストbind-usersに、この制限に起因する問題が数件投稿
- ゾーン頂点のTXTレコード数がdefaultの上限数100に到達する可能性
  - SPFレコードの名前解決失敗により、メールの送信ドメイン認証に影響を与える可能性

対策となりえるI-D

- Upper limit values for DNS 共通のレコード数上限値が必要。
- Domain Control Validation using DNS ゾーン頂点にTXTレコードを置かない。

これからの(個人的な)課題

- それぞれのフルリゾルバに制限されない項目があるため継続調査

	対策(新しい制限)	制限されない項目
BIND	RRsetのレコード数の制限 (default: 100)	ラベル数、名前圧縮に制限なし
PowerDNS Recusor	RRsetのレコード数の制限 (default: 256)	ラベル数、名前圧縮に制限なし
Unbound	名前圧縮の回数制限(120)	RRsetのレコード数に制限なし
Knot Resolver	性能改善のみで新しい制限はなし	RRsetのレコード数に制限なし ラベル数、名前圧縮に制限なし

これからの(個人的な)課題

- 権威サーバ
  - セカンダリサービスなど他者がゾーンを自由に設定できるサービス
  - NSD
  - PowerDNS Authoritative Server
  - Knot DNS
  - YADIFA

- DNSクライアント
  - 非常に多いレコード数のRRsetがある場合のDNSクライアントの動作
  - 例：Postfix stable release 3.8.6, and legacy releases 3.7.11, 3.6.15, 3.5.25
    - 宛先のドメイン名のMXレコードとそのAレコードが非常に多い場合、メール送信プロセス(postfix/smtp)がStack領域を使い切り異常終了。

まとめ

- レコード数のRRsetを利用することで、フルリゾルバの性能を低下することができる問題が存在した。
- その対策により一部のフルリゾルバでは、レコード数の制限が導入されたが、その影響が懸念される。
- レコード数のRRsetの問題は、今後も調査予定。