PowerDNSで遊んでみた。

坂口　俊文（個人参加）

DNS Summer Days 2015

2015/07/24

資料公開のため修正

概要

PowerDNS Security Advisory 2015-01

(CVE-2015-1868/CVE-2015-5470)

https://doc.powerdns.com/md/security/powerdns-advisory-2015-01/

http://jprs.jp/tech/security/2015-04-27-powerdns-vuln-decompression.html

以下の2点についてアナウンス

- 4/23: 特定のプラットフォーム(RedHat/CentOS 5.x)にて、細工したドメインを用意し、そのドメインに関するクエリを送信することで、PowerDNSがクラッシュ。
- 5/1, 7/7: すべてのプラットフォームにて、細工したクエリを送信することで、サーバのCPU負荷が急上昇。

本日は、後者について発表します。

自己紹介

坂口　俊文

- ２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？
- 本日は個人参加
- Twitter: @siskrn
- GitHub: https://github.com/sischkg/
- PowerDNS歴: ちょうど3ヶ月（2015/7/24時点）

最近、ここに名前が乗りました。

PowerDNS Security Advisory 2015-01: Label decompression bug can cause crashes or CPU spikes

- CVE: CVE-2015-1868
- Date: 23rd of April 2015
- Credit: Aki Tuomi, Toshifumi Sakaguchi
- Affects: PowerDNS Recursor versions 3.5 and up; Authoritative Server 3.2 and up
- Not affected: Recursor 3.6.3; Recursor 3.7.2; Auth 3.3.2; Auth 3.4.4
- Severity: High

経緯(CVE-2015-1868)

4/23 にセキュリティアドバイザリが公開。内容は、

"ドメイン名の圧縮の展開の不具合により、特定のプラットフォーム(RedHat/CentOS 5.x)にて、プロセスがクラッシュ。"

であるため、検証していたところ、

"**CentOS 6.6でも**PowerDNS Recursor 3.6.2でCPU使用率が上昇"

となる現象を発見。→PowerDNSの開発元へ報告(4/29)。

影響(CVE-2015-1868)

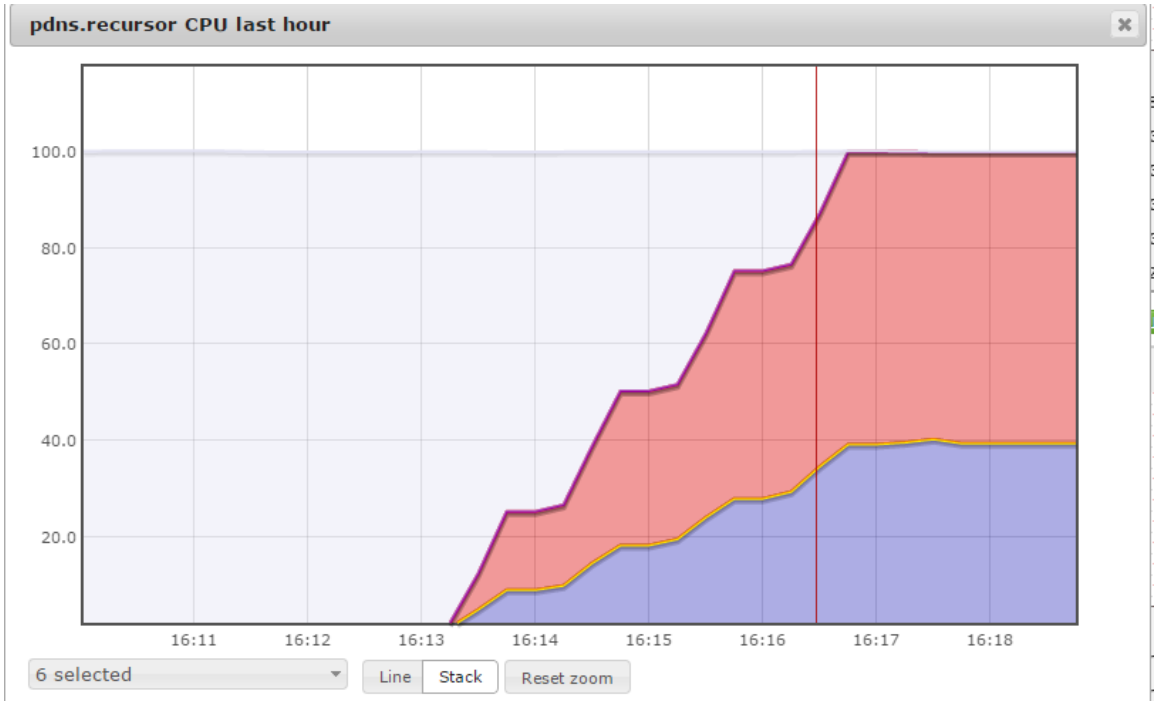
細工したUDPクエリをPowerDNSへ送信

ひとつのクエリで、論理CPUのひとつの使用率が100%

そのクエリが、PowerDNSのひとつのThreadを占有（1,2分）

Thread数のクエリで、PowerDNSは無応答に

影響(CVE-2015-1868)



一定間隔でクエリを受信したときのCPU使用率

- 4論理CPUサーバ
- CentOS 6.6
- PowerDNS Recursor 3.6.2

対象の環境(CVE-2015-1868)

アドバイザリには記載はないが、影響が出る環境と出ない環境が存在

影響がでた環境

- PowerDNS Recursor 3.6.2

  CentOS 5.11, 6.6
- PowerDNS Authoritative Server 3.4.3

  CentOS 6.6

影響がでなかった環境

- PowerDNS Recursor 3.7.1

  CentOS 6.6

原因(CVE-2015-1868)

PowerDNS Authoritative Server 3.4.3/Recursor 3.6.2では以下の問題が存在するため、CPU負荷の上昇が発生。

- ドメイン名の長さが無制限
  → 256文字以上もエラーにならない
- ドメイン名の圧縮を展開する際の問題
  → 自己参照で無限ループ
  → ループ対策のリミッタが大きい(1000)
- DNSメッセージ内のドメイン名を文字列に変換する際の、余計な処理
  → std::string::reserve storm.

原因となるSource Code(CVE-2015-1868)

pdns/dnsparser.cc内のメンバ関数

void PacketReader::getLabelFromContent(…)

DNSメッセージ内のドメイン名

文字列

```
456  void PacketReader::getLabelFromContent(const vecto
457  {
458    if(recurs > 1000) // the forward reference-check
459      throw MOADNSException("Loop");
460    for(;;) {
461      unsigned char labellen=content.at(frompos++);
462
463      if(!labellen) {
464        if(ret.empty())
465                ret.append(1,'.');
466        break;
467      }
468      else if((labellen & 0xc0) == 0xc0) {
469        uint16_t offset=256*(labellen & ~0xc0) + (un
470        //        cout<<"This is an offset, need to
471
472        if(offset >= frompos-2)
473          throw MOADNSException("forward reference d
474        return getLabelFromContent(content, offset,
475      }
476
```

https://github.com/PowerDNS/pdns/blob/rec-3.6.2/pdns/dnsparser.cc
https://github.com/PowerDNS/pdns/blob/auth-3.4.3/pdns/dnsparser.cc

getLabelFromContentの処理

```
getLabelFromContent (  ... string  &ret... ) {  // retは、処理後のドメイン名の保存先
   if 再起呼び出しが1000を超えた  {  例外をthrow   }
   for(;;) {
      DNSメッセージ内のドメイン名から1byte（ラベル長）を取得

      if  ラベル長 == 0(ドメイン名を全て処理）  {   終了   }

      if  ラベル長 & 0xC0  (ドメイン名圧縮)  {
         if  前方参照   {  例外をthrow   }
        参照先を指定して、getLabelFromContentを再帰呼び出し
      }

      ラベルを取得 し、retへ追記
   }
}
```

std::string::reserve storm

Authoritative Server 3.4.3およびRecursor 3.6.2では、ひとつのラベルを読み込む前に、一回std::string::reserveを呼ぶ。

```
// XXX FIXME THIS MIGHT BE VERY SLOW!
ret.reserve(ret.size() + labellen + 2);
for(string::size_type n = 0 ; n < labellen; ++n, frompos++) {
  if(content.at(frompos)=='.' || content.at(frompos)=='\\') {
    ret.append(1, '\\');
    ret.append(1, content[frompos]);
  }
  else if(content.at(frompos)==' ') {
    ret+="\\032";
  }
  else
    ret.append(1, content[frompos]);
```

Recursor 3.7.1では、std::string::reserveを削除済み。

std::string::reserve storm

この一行を追加するだけで、実行時間に致命的な差が発生

Auth 3.4.3/Recursor 3.6.2

```
std::string ret;
for ( int i = 0 ; i < MAX ; i++ ) {
   ret.reserve( ret.size() + n );
   ret.append( label );
   ret.append( "."   );
}
```

実行時間: **45.5秒**

Recursor 3.7.1

```
std::string ret;
for ( int i = 0 ; i < MAX ; i++ ) {

   ret.append( label );
   ret.append( "."  );
}
```

>>>>　実行時間: 0.01秒

* 実行環境：CentOS 5.11　on VirtualBox; CPU Core i5 2510M 2.5GHz
* std::string::reserveの実装によっては、結果が異なる。

対策(CVE-2015-1868)

PowerDNSの開発元は、以下のバージョンへのアップグレードもしくは、パッチの適用を推奨

- PowerDNS Authoritative 3.4.4
- PowerDNS Recursor 3.6.3
- PowerDNS Recursor 3.7.2

修正内容

	ドメイン名の長さ制限	ドメイン名圧縮の展開の不具合	std::string::reserve
Auth 3.4.3 →3.4.4	制限なし	**自己参照を禁止 再帰制限1000→100**	有
Recursor 3.6.2→3.6.3	制限なし	**自己参照を禁止 再帰制限1000→100**	有
Recursor 3.7.1→3.7.2	制限なし	**自己参照を禁止 再帰制限1000→100**	元から無

ドメイン名の長さ制限の欠如の影響

- 修正内容において、ドメイン名の長さを制限していなかったため、もう少し調査

→ PowerDNS Authoritative Server 3.4.4で問題を発見

→ PowerDNS開発元に報告（5/22)

→ CVE-2015-5470

ドメイン名の長さ制限の欠如の影響

(CVE-2015-5470)

Authoritative Server 3.4.4に対して、TCPで細工したDNSクエリを送信。

- ドメイン名圧縮は関係なし

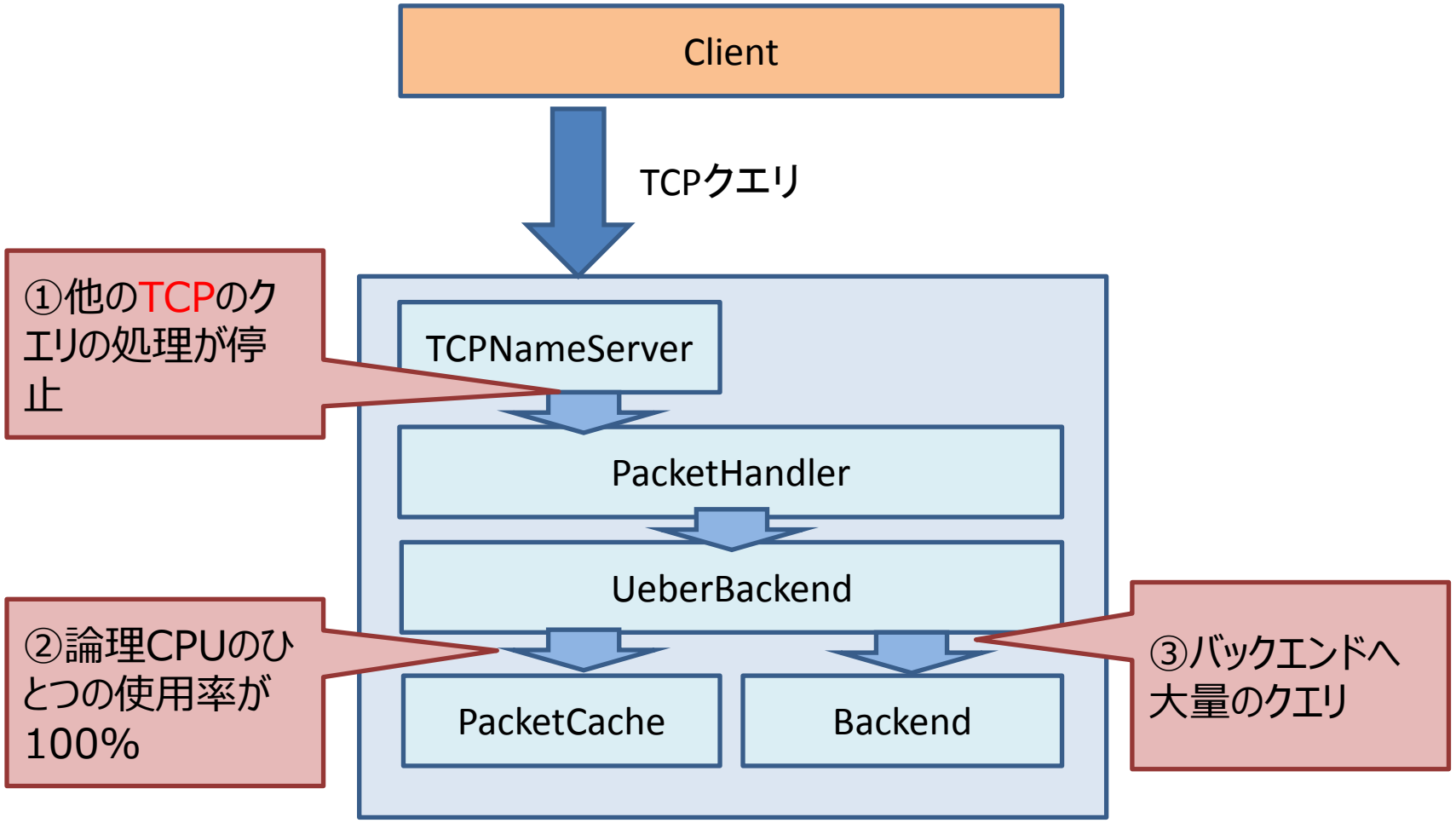
影響(CVE-2015-5470)

- ひとつのクエリで論理CPUのひとつの使用率が100%
（複数のクエリで複数のCPUの使用率が上がることはない）

- 他のTCPのクエリの処理が停止
（UDPのクエリには影響なし）
- バックエンド(MySQLなど)へ大量のクエリ

- PowerDNS Authoritative 3.4.4以下で発生
- PowerDNS Recursorでは影響なし

PowerDNS Authritative Serverの処理



http://blog.powerdns.com/2015/06/23/what-is-a-powerdns-backend-and-how-do-i-make-it-send-an-nxdomain/

他のTCPクエリの処理が停止

TCPクエリの場合、PacketHanderへ処理を移す前にLockを取得する。そのため、その処理が終わるまで他のTCPクエリは、Lockの開放を待つ。

```
if(logDNSQueries)
    L<<"packetcache MISS"<<endl;
{
  Lock l(&s_plock);
  if(!s_P) {
    L<<Logger::Error<<"TCP server is without backend connecti
    s_P=new PacketHandler;
  }
  bool shouldRecurse;

  reply=shared_ptr<DNSPacket>(s_P->questionOrRecurse(packet.g
```

https://github.com/PowerDNS/pdns/blob/auth-3.4.4/pdns/tcpreceiver.cc

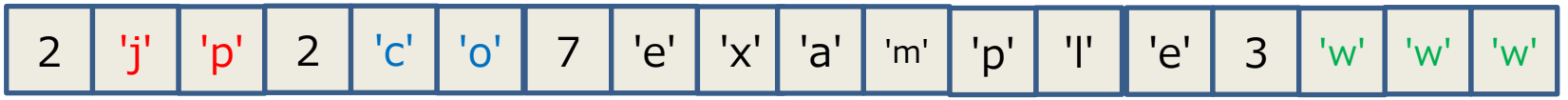
論理CPUのひとつの使用率が100%

1. 最初にqnameのSOAをPacketCacheから検索
2. 見つからない場合は、先頭のラベルを削除してもう一回
3. 見つけるまで繰り返す
4. 最後まで見つからなければ、バックエンドから検索

www.example.co.jp
example.co.jp
co.jp
jp

さらに、PacketCacheではドメイン名を次のように変換して扱う。

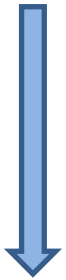
www.example.co.jp



バックエンドへの大量のクエリ

1. qnameのSOAをバックエンドから検索
2. 見つからない場合は、先頭のラベルを削除してもう一回
3. 見つけるまで繰り返す。

www.example.co.jp
example.co.jp
co.jp
jp



Backendへ大量のクエリが発生

対策(CVE-2015-5470)

PowerDNSの開発元は、6/9に新バージョンをリリース。

- PowerDNS Authoritative 3.4.5
- PowerDNS Recursor 3.6.4
- PowerDNS Recursor 3.7.3

Bug fixes: Limit the maximum length of a qname

修正内容

	ドメイン名の長さ制限	ドメイン名圧縮の展開の不具合	std::string::reserve
Auth 3.4.3→3.4.5	**制限なし→制限あり (1024未満)**	**自己参照を禁止 再帰制限1000→100**	**あり→なし**
Recursor 3.6.2→3.6.4	**制限なし→制限あり (1024未満)**	**自己参照を禁止 再帰制限1000→100**	あり→あり
Recursor 3.7.1→3.7.3	**制限なし→制限あり (1024未満)**	**自己参照を禁止 再帰制限1000→100**	なし→なし

まとめ

- 以下のバージョンのPowerDNSは、外部からの攻撃によりサービスが停止

✓ Authoritative Server 3.4.4以下

✓ Recursor 3.6.2以下

- Exploitは簡単に作成可能

✓ アドバイザリやパッチの内容で十分作成可能

✓ CVE-2015-1868→３時間かかりませんでした

✓ CVE-2015-5470→MySQL（バックエンド）のクエリログを見れば…