DNS(OSS, サーバー)ソフトウェアの変化

IIJ
Internet Initiative Japan

株式会社
インターネットイニシアティブ
島村 充
<simamura@iij.ad.jp>

Ongoing Innovation

本日取り上げるDNSサーバーソフトウェア

- BIND9
- NSD
- Unbound
- Power DNS Authoritative Server
- Power DNS Recursor
- Knot DNS
- Knot Resolver

BIND9

おさらい: BIND9のversioning

- **開発版: 奇数系 (9.13, 9.15, …)**
  - 現在の最新は 9.15.6
- **安定版: 偶数系 (9.14, 9.16, …)**
  - 現在の最新は 9.14.8
- **ESV(Extended Support Version): 9.11**
  - 4年間のサポート
  - 9.11は2021年12月までサポート
  - 次のESVは9.16 (‘20 Q1リリース予定)

BIND 9.11

- **昨年のIW時点: 9.11.5 (2019/10/18リリース)**
- **12/12 9.11.5-P1**
  - NSEC(3)関連の不具合の修正
- **02/21 9.11.5-P4**
  - 複数のEDNS keytagオプションのあるパケットの処理でメモリリークする脆弱性
  - Trust Anchorの自動更新で、更新後のTAのアルゴリズムが未対応のものだった場合にcrashする脆弱性
  - DLZを利用している場合に、意図していないゾーン転送を行ってしまう脆弱性

BIND 9.11

- **02/28 9.11.6**
  - bugfix中心
- **04/24 9.11.6-P1**
  - tcp-clientsが効かず、file descriptorが溢れてしまうDoS
- **05/16 9.11.7**
  - bugfix中心
- **06/19 9.11.8**
  - 名前解決の際に異常なパケットを破棄するタイミングでrace conditionでcrash

BIND 9.11

- **07/17 9.11.9**
  - GeoIP2 API対応
  - 他bugfix
- **08/21 9.11.10**
  - bugfix中心
- **09/18 9.11.11**
  - bugfix中心

BIND 9.11

- **10/16 9.11.12**
  - bugfix中心
- **11/20 9.11.13**
  - TCP pipeliningを用いると、TCPの同時接続数の制限がバイパスされてDoS

BIND 9.11

- **サマリ:**
  - ◆TCP周りのDoSの修正に苦戦
  - ◆脆弱性以外もかなり頻繁な更新
    - ✓ほとんどbugfix
    - ✓“-PX” は止めたのか？

[DNSOPS dnsops 1685] Re: （緊急1件）BIND 9の脆弱性に関する注意喚起の公開について

先日、ISCから「今年から可能な限り、11/1-12/31に緊急でない
セキュリティイシューの公開をスケジュールするのを避ける」という
旨のアナウンスが公開されましたが[*1]、それでも出たということで。。

[*1] ISC Security Vulnerability Policy Updated
<https://www.isc.org/blogs/vulnerability-policyupdate/>

BIND 9.14

- **2019/03/22 9.14.0リリース**
- **New Feature**
  - EDNS workaround削除 (DNS Flag Day (2019))
  - QNAME minimisation有効化 (relaxed mode)
  - mirror zone
  - root key sentinel
  - min-cache-ttl/min-ncache-ttl
- **Linuxでbuild時に(デフォルトでは)libcapが必要に**

BIND 9.14

- **9.14固有の脆弱性**
- **9.14.0:**
  - nxdomain-redirectを使っていると特定条件でcrashする
- **～9.14.6:**
  - QNAME minimisationを有効化しており、forwarderがreferralを返すとcrashする
  - mirror zoneを使っている際に、それに対するDNSSEC検証をバイパスすることができる場合がある

いつもの「新機能実装→脆弱性」の流れ

NSD

NSD

- **去年のIW時点: 4.1.25 (2018/09/25リリース)**
- **12/04 4.1.26**
  - DNSTAPサポート
  - FreeBSD12でSO_REUSEPORT_LBを使えるように
- **03/25 4.1.27**
  - deny-any導入＆デフォルト有効
- **06/11 4.2.0**
  - hide-identityオプション導入
  - TLS OCSP staplingサポート

NSD

- **07/09 4.2.1**
  - bugfix中心
- **08/19 4.2.2**
  - 細工されたゾーンファイルを読み込むとcrash
- **11/20 4.2.3**
  - 異なるゾーンが同居しているときに、不必要にchainを辿らないようにするオプション(confine-to-zone)

NSD

- **サマリ:**
  - ◆DNSTAP導入
  - ◆deny-anyがデフォルト有効で導入された
  - ◆久しぶりのCVE
    - ✓ただし、remoteからは不可

Unbound

Unbound

- **去年のIW時点: 1.8.1 (2018/10/08リリース)**
- **12/04 1.8.2**
  - deny-any実装
- **12/11 1.8.3**
  - DNS64のbug fix
- **02/05 1.9.0**
  - EDNS workaround削除(DNS Flag Day (2019))
  - DoTのTLS関連オプション追加

Unbound

- **03/11 1.9.1**
  - ログ周りの改善
- **06/17 1.9.2**
  - [AI]XFR over TLS
  - deny-anyの応答がNOTIMPを返すようになる
- **08/27 1.9.3**
  - IPSet module導入(iptablesと協調するための応答を返すmodule)
  - crashバグ修正

Unbound

- **10/03 1.9.4**
  - 細工されたNOTIFYを受信するとcrashする脆弱性
- **11/19 1.9.5**
  - ipsec moduleを有効にしている際に、細工された IPSECKEY応答を受け取ると**shell code実行が可能な脆弱性**
- **サマリ:**
  - EDNS workaround削除
  - deny-any
  - 脆弱性多め。しかもRemote Code実行有(not default)

PowerDNS Authoritative Server

PowerDNS Authoritative Server 4.0.x

- **去年のIW時点: 4.0.6 (2018/11/06リリース)**
- **03/18 4.0.7**
  - HTTPリモートバックエンドでバリデーションが不十分だった
- **06/21 4.0.8**
  - 細工されたレコードのあるゾーンを読み込むことによってクラッシュ
  - 多数のNOTIFYを送られることでCPU負荷が上がってしまう

PowerDNS Authoritative Server 4.0.x

- **08/01 4.0.9**
  - PostgreSQLバックエンドを使っている際に、細工されたレコードのあるゾーンを読み込むことによりクラッシュ
- **サマリ:**
  - crashバグ2件

PowerDNS Authoritative Server 4.1.x/4.2.0

- **去年のIW時点: 4.1.5 (2018/11/06リリース)**
- **01/31 4.1.6**
  - 同一の名前に対して、CNAME/SOAレコードを1つに制限
- **03/18 4.1.7**
  - HTTPリモートバックエンドでバリデーションが不十分だった
- **03/22 4.1.8**
  - bugfix中心

PowerDNS Authoritative Server 4.1.x/4.2.0

- **06/19 4.1.9**
  - “superslave” を無効化できるように
- **06/21 4.1.10**
  - 細工されたレコードのあるゾーンを読み込むことによってクラッシュ
  - 多数のNOTIFYを送られることでCPU負荷が上がってしまう

PowerDNS Authoritative Server 4.1.x/4.2.0

- **08/01 4.1.11**
  - PostgreSQLバックエンドを使っている際に、細工されたレコードのあるゾーンを読み込むことによりクラッシュ
- **08/09 4.1.13**
  - bugfix中心
- **08/30 4.2.0**
  - LMDBバックエンド
  - “LUA” RR Type
  - 他多数

PowerDNS Authoritative Server 4.1.x/4.2.0

- **サマリ:**
  - 4.2.0で “LUA” RR Typeが導入
    - ✓PowerDNS Recursor 4.0.0に続き。

Power DNS Recursor

Power DNS Recursor

- **去年のIW時点: 4.1.8 (2018/11/26リリース)**
- **01/21　4.1.9**
  - TCPで問い合わせされた際にLUA scripの呼び出しがバイパスされる場合がある脆弱性
  - DNSSEC validationをバイパス可能性な脆弱性
- **01/24　4.1.10**
  - protobufサポートを無効にしてbuildした場合のbugfix
- **02/01　4.1.11**
  - protobuf口ギング有効時のsystem callの利用の削減
    - ✓Spectre/Meltdown対策への対策

Power DNS Recursor

- **04/02　4.1.12**
  - EDNS Client Subnet利用時のキャッシュ上限を実装
- **05/21　4.1.13**
  - wildcardなレコードに対するDNSSEC検証のbugfix
- **06/13　4.1.14**
  - bugfix
- **07/16　4.2.0**
  - EDNS workaround削除 (DNS Flag Day (2019))

Power DNS Recursor

- **サマリ:**
  - ◆EDNS workaround削除は結構遅めだった
    - ✓7/16 4.2.0

Knot DNS

Knot DNS

- **去年のIW時点: 2.7.4 (2018/11/13リリース)**
- **11/11 2.9.1**
  - bugfix中心
- **10/10 2.9.0**
  - tcp-reuseportサポート
- **09/24 2.8.4**
  - DSレコードをDDNSを利用して親ゾーンにアップロードする機能

Knot DNS

- **07/16 2.8.3 | 07/15 2.7.8**
  - TCP clientの上限に達したときのCPU負荷の低減
- **06/05 2.8.2**
- **04/09 2.8.1 | 04/08 2.7.7**
- **03/05 2.8.0**
- **01/23 2.7.6**
- **01/07 2.7.5**

Knot Resolver

Knot Resolver

- **去年のIW時点: 3.1.0 (2018/11/02リリース)**
- **10/07 4.2.2**
- **09/26 4.2.1**
- **08/05 4.2.0**
  - RD bitが立っていない問い合わせにREFUSEDを返す
- **07/10 4.1.0**
  - 偽の不在応答を返す脆弱性
  - DNSSEC署名されたドメインをinsecureにダウングレードさせることのできる脆弱性

Knot Resolver

- **04/18 4.0.0**
  - DNSSEC検証がデフォルト有効化
  - DoTのportのlistenがデフォルト有効化
  - DoHサポート
- **01/10 3.2.1**
- **12/17 3.2.0**