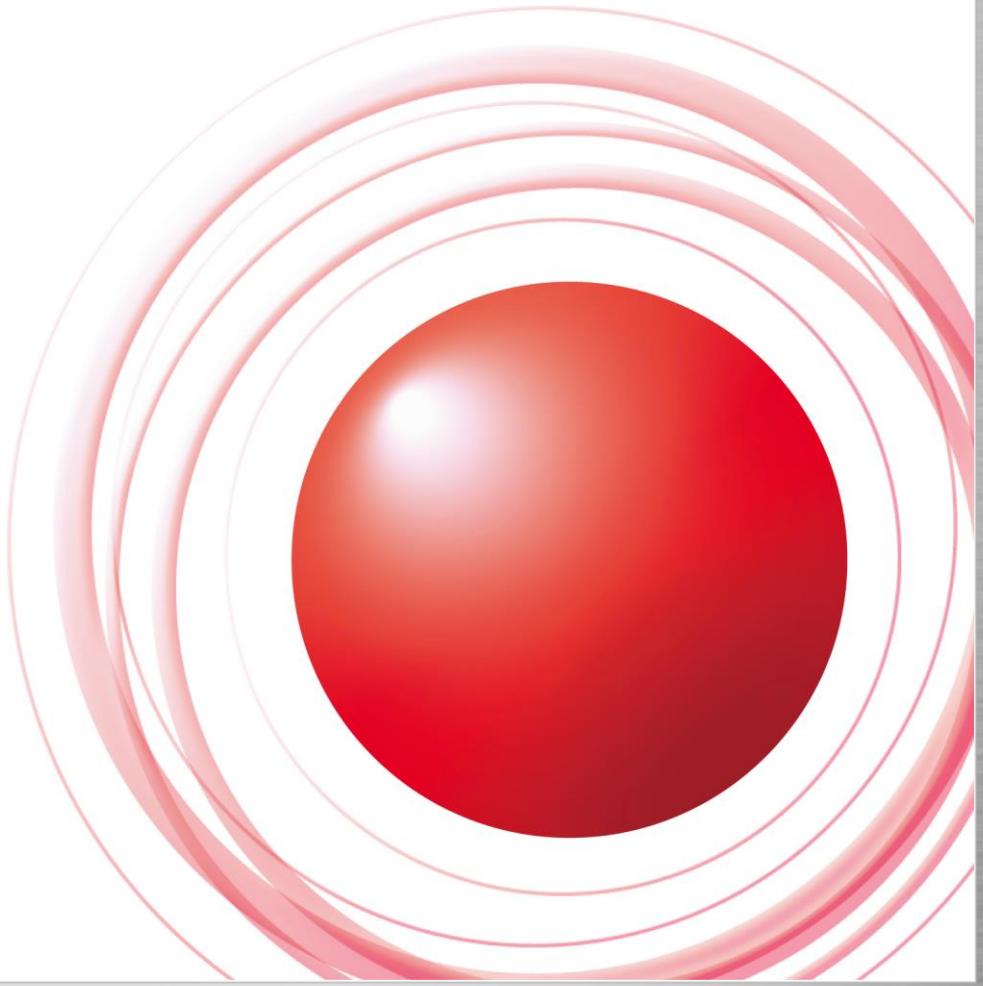
BINDからの卒業

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

BINDからの卒業?

- BINDの問題点
  - DoS脆弱性多すぎなんだよおおおおおおおお
  - 「重複」に怯える日々。「夏のBIND祭り」

	1	2	3	4	5	6	7	8	9	10	11	12
2009							◎					
2010							◎					◎
2011		◎			○	◎	◎					◎/○
2012						◎	○		◎	◎		○
2013	○		◎			◎	◎					
2014	◎				◎	◎						○/◎
2015		◎					◎/◎		◎			◎
2016	◎		◎									

※ JPRSさん「DNS関連技術情報」にて“(重要)”→◎ 無印→○
同日公開のものは1つにまとめてある

BINDの脆弱性について

- Security Architecture of BIND 9
  - JANOG US Regional Meeting #2での神明さんの発表
  - BIND9はBIND8に比べると遥かにマシ
  - BIND8のコードを再利用しない
    (デザインしなおし)
    - “16 buffer overflow/overrun bugs in changelog of BIND 8.4.7”
    - BIND9ではRemote Code Executionなし
      - でも落ちる!
  - 2000/09/16 9.0.0リリース
    - いろいろ古い…

BINDの脆弱性の分析

- CHANGESに65個の “[security]”
- BIND 9 Security Vulnerability Matrix に56のCVE-ID
- 神明さん分析
  - 28(or 29)のassertion failure
  - メモリリーク1, 無限ループ1
- JPRSさんの「DNS関連技術情報」にて
  - BIND9の脆弱性
    - “（緊急）” 25件
    - “（緊急）” ではないもの12件

      (2005年～)

BINDの脆弱性の特徴

- RCEはない
- assert() (INSIST, REQUIRE) でプロセスが死ぬ
- メモリリーク、無限ループ (リソース食いつぶし)
- ACLが意味を成さない (ACLを解釈する前段階で死ぬ)
- その機能を使っていなくても死ぬ場合がある
  (DNSSEC, Dynamic Update(DDNS))
- 外部からのpacket 1発で死ぬものがある
  - 通称: BINDコロリ(CVE-2009-0696 BIND Dynamic Update DoS)
- 外部からpacketが届かなくても死ぬものがある
  - 特定の名前を引か(さ)れてしまうとOUT
    - CVE-2012-4244,CVE-2013-2266,CVE-2015-5986など

BINDの脆弱性の特徴

- RCEはない (再)
  - コード実行されないなら、即座に自動起動されるようにしてれば、たいして影響なくね??
  - systemd, runsv, monit, contrib/scripts/nanny.pl
  - 起動が早くなったとはいえ、やはりある程度は時間がかかる
    - 権威サーバーで5万ゾーンで10分超とか
      - その間応答しないゾーンがある
    - cacheでも(良くても)2秒位は応答しない
    - パケット一発で死ぬような脆弱性がある
      - 送り続けると…? 当然ずっと応答しない

BINDの脆弱性の原因

- BIND9のコードは割とどうしようもない
  - 保護機構がないから? プログラマの質?
    - すごくいろんなところで使われているので、crash bugがみつかりやすい?

      (他のソフトでは見つかっていないだけ?)
  - 新機能追加 → crash bug発見のループ
    - RPZ(2.5回), DNS64(2.5回), prefetch, GeoIP, OPENPGPKEY RR, DNS Cookie
  - 網羅的なテストがないとおもわれる
    - RPZ有効時に、くべているドメインのRRSIGを引くだけで落ちる など
    - 発見されたバグに対してピンポイントのテストは追加されている

BINDの脆弱性の原因

- 複雑なモノリシックアーキテクチャ
  - 権威・キャッシュ同居
  - Dynamic Update
  - 個々のスレッドが密接に絡まっており、1スレッドだけ死ぬというのは無理
    - イベントドリブン?なにそれ?おいしいの?(16年前のソフトです)

BINDの脆弱性の原因

- RDATAを解釈している
  - NAPTRで正規表現解釈して死亡
  - APL, OPENPGPKEY解釈して死亡
  - 新しいRR Typeが次々に追加される
    - SPFレコードの失敗の反省から?
  - **新しいRDATAの対応はESV系列にも入る**
    - ESVを使っていて、新機能はいらないだろうと安心していても、昔々からあるわけではないような脆弱性でも影響を受ける可能性がある

BINDの脆弱性の原因

-

TYPE	Value	Meaning	Reference	Template	Registration Date
AVC	258	Application Visibility and Control	[Wolfgang_Riedel]	AVC/avc-completed-template	2016-02-26
SMIMEA	53	S/MIME cert association	[draft-ietf-dane-smime]	SMIMEA/smimea-completed-template	2015-12-01
CSYNC	62	Child-To-Parent Synchronization	[RFC7477]		2015-01-27
OPENPGPKEY	61	OpenPGP Key	[RFC-ietf-dane-openpgpkey-12]	OPENPGPKEY/openpgpkey-completed-template	2014-08-12
CDNSKEY	60	DNSKEY(s) the Child wants reflected in DS	[RFC7344]		2014-06-16
EUI64	109	an EUI-64 address	[RFC7043]	EUI64/eui64-completed-template	2013-03-27
EUI48	108	an EUI-48 address	[RFC7043]	EUI48/eui48-completed-template	2013-03-27
CDS	59	Child DS	[RFC7344]	CDS/cds-completed-template	2011-06-06
CAA	257	Certification Authority Restriction	[RFC6844]	CAA/caa-completed-template	2011-04-07
URI	256	URI	[RFC7553]	URI/uri-completed-template	2011-02-22
TALINK	58	Trust Anchor LINK	[Wouter_Wijngaards]	TALINK/talink-completed-template	2010-02-17
RKEY	57	RKEY	[Jim_Reid]	RKEY/rkey-completed-template	2008-01-21
NINFO	56	NINFO	[Jim_Reid]	NINFO/ninfo-completed-template	2008-01-21
TA	32768	DNSSEC Trust Authorities	[Sam_Weiler] [http://cameo.library.cmu.edu/][		2005-12-13

「N」が

最近のBINDの脆弱性

- american fuzzy lop の登場 (もふもふ)
  - GAを使ってテストケースを変更して、カバレッジを上げるファジングツール
    - CVE-2015-5477: An error in handling TKEY queries can cause named to exit with a REQUIRE assertion (2015/07/28)
    - CVE-2015-5986: An incorrect boundary check can trigger a REQUIRE assertion failure in openpgpkey_61.c (2015/09/03)
    - CVE-2015-5722: Parsing malformed keys may cause BIND to exit due to a failed assertion in buffer.c (2015/09/03)
  - その他多数の犠牲者たち…
    - Shellshockとか…

最近のBI

- americar
  - GAを
    レッシ
    - CVE
      caus
    - CVE
      REQ
    - CVE
      to e
  - その他多
    - Shel

IJG jpeg [1]	libjpeg-turbo [1] [2]	libpng [1]
libtiff [1] [2] [3] [4] [5]	mozjpeg [1]	PHP [1] [2] [3] [4] [5]
Mozilla Firefox [1] [2] [3] [4]	Internet Explorer [1] [2] [3] [4]	Apple Safari [1]
Adobe Flash / PCRE [1] [2] [3] [4]	sqlite [1] [2] [3] [4]…	OpenSSL [1] [2] [3] [4] [5] [6] [7]
LibreOffice [1] [2] [3] [4]	poppler [1]	freetype [1] [2]
GnuTLS [1]	GnuPG [1] [2] [3] [4]	OpenSSH [1] [2] [3]
PuTTY [1] [2]	ntpd [1]	nginx [1] [2] [3]
bash (post-Shellshock) [1] [2]	tcpdump [1] [2] [3] [4] [5] [6] [7] [8] [9]	JavaScriptCore [1] [2] [3] [4]
pdfium [1] [2]	ffmpeg [1] [2] [3] [4] [5]	libmatroska [1]
libarchive [1] [2] [3] [4] [5] [6]…	wireshark [1] [2] [3]	ImageMagick [1] [2] [3] [4] [5] [6] [7] [8]…
BIND [1] [2] [3]…	QEMU [1] [2]	lcms [1]
Oracle BerkeleyDB [1] [2]	Android / libstagefright [1] [2]	iOS / ImageIO [1]
FLAC audio library [1] [2]	libsndfile [1] [2] [3] [4]	less / lesspipe [1] [2] [3]
strings (+ related tools) [1] [2] [3] [4] [5] [6] [7]	file [1] [2] [3] [4]	dpkg [1] [2]
rcs [1]	systemd-resolved [1] [2]	libyaml [1]
Info-Zip unzip [1] [2]	libtasn1 [1] [2]…	OpenBSD pfctl [1]
NetBSD bpf [1]	man & mandoc [1] [2] [3] [4] [5]…	IDA Pro [reported by authors]
clamav [1] [2] [3] [4] [5]	libxml2 [1] [2] [4] [5] [6] [7] [8] [9]…	glibc [1]
clang / llvm [1] [2] [3] [4] [5] [6] [7] [8]…	nasm [1] [2]	ctags [1]
mutt [1]	procmail [1]	fontconfig [1]
pdksh [1] [2]	Qt [1]	wavpack [1]
redis / lua-cmsgpack [1]	taglib [1] [2] [3]	privoxy [1] [2] [3]

、カバ

eries can
(2015/07/28)
can trigger a
(2015/09/03)
cause BIND
5/09/03)

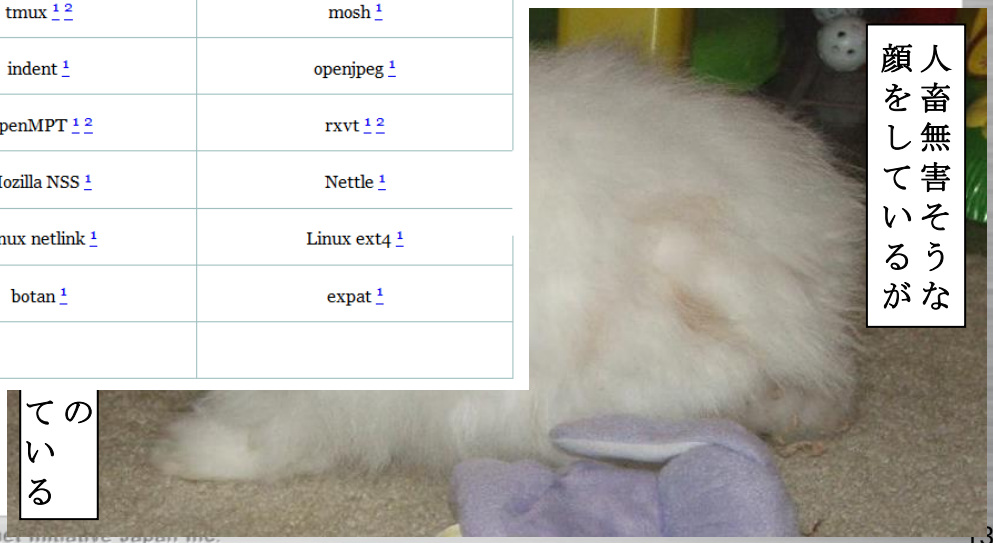
最近のBINDの脆弱性

- american fuzzy lop の登場（たぶん）
  - GAを
    - CVE
      caus
    - CVE
      REQ
    - CVE
      to e
  - その他多
    - Shel

て、カバ

ueries can
n (2015/07/28)
can trigger a
c (2015/09/03)
y cause BIND
15/09/03)

perl [1] [2] [3] [4] [5] [6] [7]...	libxmp	radare2 [1] [2]
SleuthKit [1]	fwknop [reported by author]	X.Org [1] [2]
exifprobe [1]	jhead [?]	capnproto [1]
Xerces-C [1] [2]	metacam [1]	djvulibre [1]
exiv [1]	Linux btrfs [1] [2] [3] [4] [6] [7] [8]	Knot DNS [1]
curl [1] [2]	wpa_supplicant [1]	libde265 [reported by author]
dnsmasq [1]	libbpg [1]	lame [1]
libwmf [1]	uudecode [1]	MuPDF [1]
imlib2 [1]	libraw [1]	libbson [1]
libsass [1]	yara [1] [2] [3] [4]	W3C tidy-html5 [1]
VLC [1]	FreeBSD syscons [1] [2] [3]	John the Ripper [1] [2]
screen [1] [2] [3]	tmux [1] [2]	mosh [1]
UPX [1]	indent [1]	openjpeg [1]
MMIX [1]	OpenMPT [1] [2]	rxvt [1] [2]
dhcpcd [1]	Mozilla NSS [1]	Nettle [1]
mbed TLS [1]	Linux netlink [1]	Linux ext4 [1]
Linux xfs [1]	botan [1]	expat [1]
Adobe Reader [1]		



今後の展望

- 9.11で新機能盛りだくさん
- 新しいRR TYPEがどんどん追加される
- american fussy lopパワーで今まで見つけられていなかった脆弱性がモリモリ出てくる

→ (即死)DoS脆弱性の高頻度化を予想

逃げてーーーーー

ベンダーPackageの対応状況

- 「ベンダーのサポートがないからBIND9以外使えない」とみなさんおっしゃいますが…
- 脆弱性公表からRHELパッケージリリースまで、ヤバイ脆弱性18件を調査

かかった日数	回数	運用者の気持ち
0-1日	5	早い。安心安心
2日	3	このくらいならまだ安心
3日	2	そろそろやばくね…?
4日	2	まだーー? (そろそろ攻撃が来るー)
5日	1	まだなのーーー?
6日	2	そろそろ1週間なんだけど (あわわ…)
7日	1	や、やっと出た… _(:3」∠)_
8日	1	遅いよ…
12日	1	攻撃来ないし、もう忘れかけてたわ…
13-15日	1	もうどうでもイイっす…

実際の攻撃

- 攻撃ってそんなにすぐ来ないよね?(つぶらな瞳)

来 ま す

- CVE-2015-5477: Bind TKEY Query Assertion Failure

「BIND 9」の脆弱性を狙う攻撃が発生、国内レンタルサーバー会社でアクセス不能になる被害

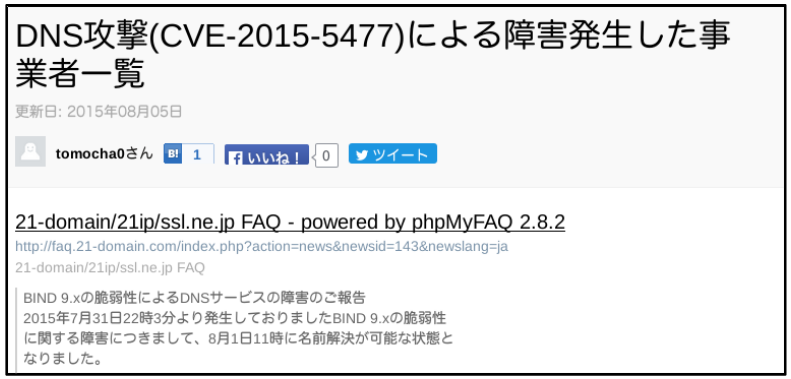
(2015/7/31 19:24)

Internet Systems Consortium（ISC）が開発・提供しているDNSソフト「BIND 9」においてサービス運用妨害（DoS）攻撃が可能な脆弱性（CVE-2015-5477）が見つかった件で、これを修正した最新バージョンへの更新または各ディストリビューターが提供する修正パッチの適用を速やかに実施するよう、株式会社日本レジストリサービス（JPRS）があらためて注意を促している。

JPRSによると、この脆弱性の実証（PoC）コードがすでにネット上で公開されており、日本国内のサービスプロバイダーからの被害事例も報告されているという。「即時の対応を強く推奨する」としている。

国内での被害としては、レンタルサーバーサービスを提供するカゴヤ・ジャパン株式会社が31日、この脆弱性に対する攻撃によって同社の権威DNSサーバーにおけるDNSサービスが停止。同日深夜に一時、名前解決が行えず、サーバーへアクセスできない障害が発生していたことを公表している。

http://internet.watch.impress.co.jp/docs/news/714526.html



2015/07/29早朝(日本時間)公開→ 7/29 AM11時「重複」→ 7/31障害

幸い、この時は7/28,29(現地時刻)にRHELのupdateがでている

実際の攻撃

- CVE-2013-4854: A specially crafted query can cause BIND to terminate abnormally (2013/07/26)

  Crashes have been reported by multiple ISC customers.
  First observed in the wild on 26 July 2013.

- CVE-2011-4313: BIND 9 Resolver crashes after logging an error in query.c (2011/11/16)

  ISC is receiving multiple reports and working with multiple customers on this issue.

- CVE-2011-1910: Large RRSIG RRsets and Negative Caching Can Crash named

  開発元であるISCは、本脆弱性の深刻度（Severity）を「高（High）」と評価しています。また、
  ・既に本脆弱性を利用した具体的な攻撃方法がインターネット上に公開されていること

実際の攻撃

- bind-users@isc.org, dns-operations@dns-oarc.netで「なんかxxxってログはいてBINDが落ちたんだけど」

CVE-2013-3919 [was Re: resolver.c:4858: fatal error]

Michael McNally mcnally at isc.org
Wed Jun 5 00:04:53 UTC 2013

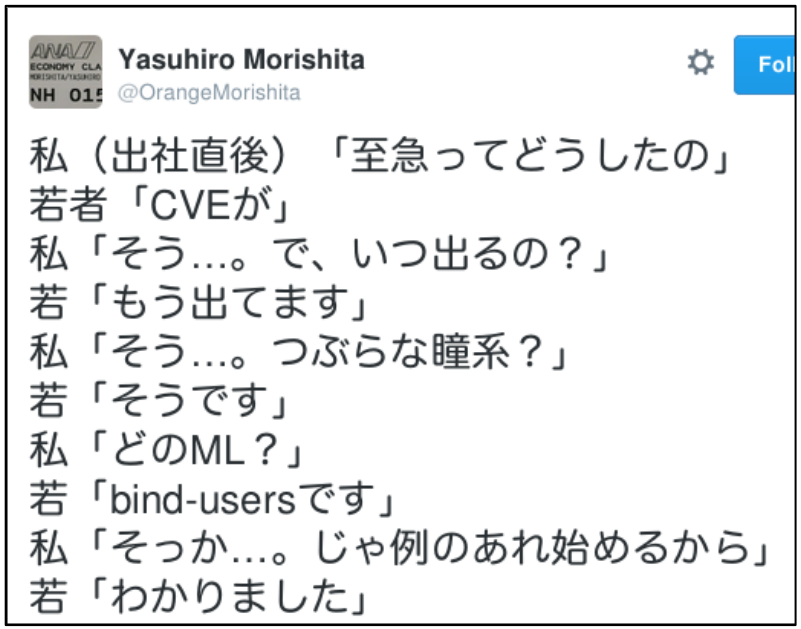
- Previous message: resolver.c:4858: fatal error
- Next message: CVE-2013-3919 [was Re: resolver.c:4858: fatal error]
- **Messages sorted by:** [date] [thread] [subject] [author]

```
On 6/4/13 1:06 AM, Stas Pirogov wrote:
> Hello,
>
> since upgrading our binds to 9.9.3 (from 9.9.2-P2) I've got
> following crash couple of times in last 3 days:
>
> 04-Jun-2013 08:33:09.531 general: critical: resolver.c:4858: fatal error:
> 04-Jun-2013 08:33:09.531 general: critical: RUNTIME_CHECK(tresult == 0)
> failed
> 04-Jun-2013 08:33:09.531 general: critical: exiting (due to fatal error in
> library)
>
> We're running various versions CentOS. This happened on both 5.3 and 5.5
>
> Please advise

Congratulations, you have discovered a bug in BIND 9.9.3, 9.8.5, and
9.6-ESV-R9.  After analyzing it and concluding that the defect was
potentially usable as a denial-of-service vector, our software
developers have produced an emergency patch release which has been
announced on the bind-announce mailing list.
```

実際の攻撃

- bind-users@isc.org, dns-operations@dns-oarc.netで「なんかxxxってログはいてBINDが落ちたんだけど」



そんなわけで…

- BIND9以外の実装に乗り換えよう!
  - BIND10はお亡くなりになりました…
    (2014/04/18 final release of BIND 10)
    - bundyと名を変えてgithubで公開されているが…

  - 実装紹介
    - Unbound:　島村
    - PowerDNS: (株)データーネット OSS研究室 大野さん
    - NSD: (株)インターネットイニシアティブ 山口さん
    - 他OSS: KnotDNS, YADIFA