CVE-2016-2848の報告

坂口　俊文

DNSOPS.JP BoF

2016/12/01

アジェンダ

BINDの脆弱性(CVE-2016-2848)をISCに報告したときの、発見者側の状況について発表します

- 自己紹介
- 経緯
- 脆弱性の発見
- 脆弱性の報告
- CVE-2016-2848の公開

自己紹介

坂口　俊文

- 3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
- 本日も個人参加
- Twitter: @siskrn
- GitHub: https://github.com/sischkg/

CVE-2016-2848の経緯

09/28（水）ISCからCVE-2016-2776の公開
09/30（金）CVE-2016-2776のPoC作成中に別の脆弱性を発見
10/01（土）ISCに脆弱性を報告
10/04（火）ISCから一次回答
10/12（水）ISCから脆弱性を確認したので対応すると回答
10/21（金）ISCからCVE-2016-2848の公開

上記のタイムゾーンはJST

CVE-2016-2776

- BIND 9.xにおける実装上の不具合により、namedに対する外部からのサービス不能（DoS）攻撃が可能となる脆弱性
- 特定の問い合わせに対応する応答メッセージのパケットを構築する際の処理でnamedが異常終了
- パケットひとつで異常終了
- フルリゾルバ及び権威DNSサーバの双方が対象
- buffer.cにおいてassertion failureが発生
- named.confでのACL(allow-queryなど)では回避できない

https://jprs.jp/tech/security/2016-09-28-bind9-vuln-rendering.html

⇒ これらの情報をもとにCVE-2016-2776のPoCを作成開始

PoCの作成(1)

1. 以下のようなDNSメッセージを送信するPoCを作成
   - QNAME → 長く
   - TSIG Key Name → 長く
   - TSIG Algorithm Name → 長く
   - OPTレコード → xxx

2. CentOS 6.8にbindパッケージ(bind-9.8.2-0.47.rc1.el6)をインストール

3. DNSメッセージを送信 ⇒ 強制終了

PoCの作成(2)

1. BINDをアップデートして、脆弱性が修正されたことを確認するため

   bind-9.8.2-0.47.rc1.el6 → bind-9.8.2-0.47.rc1.el6_8.1
2. もう一度、DNSメッセージを送信　⇒　強制終了
3. ログには、buffer.cではなくmessage.cでassertion failureと出力。別の脆弱性をついたらしい

```
message.c:2516: REQUIRE(!dns_rdataset_isassociated(*item)) failed
```

脆弱性の影響範囲の調査

Vender	OS	Version	Affected ?
ISC	CentOS 6.8	9.9.9-P3	Not affected
	CentOS 6.8	9.9.9-P2	Not affected
	CentOS 6.8	9.8.5rc2（EOL)	Not affected
	CentOS 6.8	**9.8.5rc1**（EOL)	**Affected**
	CentOS 6.8	**9.8.4-P2**（EOL)	**Affected**
CentOS Project	CentOS 7.2	9.9.4-29.el7_2.4	Not affected
	CentOS 6.8	**9.8.2-0.47.rc1.el6_8.1**	**Affected**
	CentOS 5.11	**9.7.0-21.P2.el5_11.7**	**Affected**
Canonical	**Ubuntu 12.04**	**9.8.1.dfsg.P1-4ubuntu0.17**	**Affected**

調査しない環境・バージョン

- FreeBSD(BINDはrelease 10でbaseから外れた)
- CentOS 5.x + bind9パッケージ (上記はbind97パッケージ)
- Debian

調査結果のまとめ

- 影響のあるバージョン: 9.8.5rc1以下
- 外部からDNSメッセージひとつで強制終了
- ログに”message.c:****:
  REQUIRE(!dns_rdataset_isassociated(*item)) failed”
- ISCがリリースしている現行バージョンは影響はないが、Linux Distributionが独自で管理しているパッケージは影響あり
- CVE-2016-2776のPoCを作成中に発見したため、ほかの人も発見する可能性が高い

脆弱性の報告先

9.8.xはEOL。どこに報告すればいいのか？

報告先	
ISC https://www.isc.org/downloads/software-support-policy/security-advisory/	• 報告先は一か所で済む（ISC→Linux Distributors） • 9.8.xはEOLのため取り扱わない可能性
Linux Distributors RedHat: https://access.redhat.com/security/team/contact Ubuntu: https://wiki.ubuntu.com/SecurityTeam/FAQ#Contact Debian: https://www.debian.org/security/faq#discover	• 脆弱性のあるバージョンをメンテナンスしている当事者のため必ず対応するはず • 各Distributionごとに連絡するのは大変そう（実際には連携して対応するらしい）
IPA https://www.ipa.go.jp/security/vuln/report/#contact	• 報告先は一か所で済む • 日本語を使える • 対応に時間を要する(AXFRの件では、一次回答に一か月、ISCに連絡するまでに半年)

脆弱性報告

- 10/01にISC(security-officer@isc.org)へ報告
- CVE-2016-2776のexploitを作成中にこの脆弱性を発見し、攻撃に利用する可能性があるため、スピード重視
- EOLバージョンでも、CVSSスコアが8.0以上の場合は修正
- 判断するのはISC（という口実）

ISC CVSS Scoring and Disclosure Strategy			
CVSS Base Score	Internal Description	Disclosure	Build Plan
8.0 - 10	Critical & Catastrophic	Potential Critical Notification Process	Fix all images to cover majority of deployed code (i.e. potentially open EOL images)
7.0 - 7.9	Critical	Security Advisory Required	Fix all non-EOL images
5.0 - 6.9	High	Security Advisory Required	Fix all non-EOL images
3.0 - 4.9	Medium	No Advisory Required	Fix all non-EOL images
0 - 2.9	Low	No Advisory Required	Fix in codebase and move forward

http://www.isc.org/wp-content/uploads/2013/08/CVSS_Scoring.055.jpg

CVE-2016-2776のPoC

CVE-2016-2776のPoCが公開

A TALE OF A DNS PACKET (CVE-2016-2776)

http://blog.infobytesec.com/2016/10/a-tale-of-dns-packet-cve-2016-2776.html
PoC: https://github.com/infobyte/CVE-2016-2776

PoCが公開されたことにより、

- 公開されたPoCをもとに新規の脆弱性を発見する可能性

or

- PoCが公開されたことでCVE-2016-2776の調査をやめるため、新規の脆弱性は発見されない可能性

ISCからの回答

10/04に一次回答

- 最新のバージョンでは影響ないが、どこで修正されたか興味がある
- どこで修正されたのか調査するので少し時間がほしい

10/12回答

- 過去に修正され、最新バージョンでは影響のない脆弱性を発見したときの手続きは存在しない
- 検討した結果、脆弱性をもったバージョンを使用している人がいるため、最新バージョンの脆弱性と同じ手順で公開する必要がある
- 以下のコミットで脆弱性は修正されていた

commit 4adf97c32fcca7d00e5756607fd045f2aab9c3d4
Author: Mark Andrews <marka@isc.org>
Date: Mon Apr 8 16:29:26 2013 +1000 3548.

[bug] The NSID request code in resolver.c was broken resulting
in invalid EDNS options being sent. [RT #33153]

脆弱性公開の手続き

いつ？	公開先
一般公開　3～5営業日前	ISCのサポートを受けている顧客 Rootサーバの管理者へ通知
一般公開　24時間前	OSのメンテナに通知
一般公開	メーリングリスト(bind-announce) Webサイトにて通知 JP-CERTを含む一部のCSIRTへ通知

CVE-2016-2848の公開

10/21(JST)に公開

CVE-2016-2848: A packet with malformed options can trigger an assertion failure in ISC BIND versions released prior to May 2013 and in packages derived from releases prior to that date.

Michael McNally mcnally at isc.org
Thu Oct 20 18:19:33 UTC 2016

- Previous message (by thread): BIND 9.11.0 is now available
- **Messages sorted by:** [date] [thread] [subject] [author]

CVE-2016-2848: A packet with malformed options can trigger an assertion failure in ISC BIND versions released prior to May 2013 and in packages derived from releases prior to that date.

https://lists.isc.org/pipermail/bind-announce/2016-October/001008.html

---

■（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-2848）
- フルリゾルバー（キャッシュDNSサーバー）／権威DNSサーバーの双方が対象、対象となるディストリビューション・バージョンに要注意 -

株式会社日本レジストリサービス（JPRS）
初版作成 2016/10/21（Fri）

▼概要

BIND 9.xにおける実装上の不具合により、named に対する外部からのサービス不能（DoS）攻撃が可能となる脆弱性が、開発元のISCから発表されました。本脆弱性により、提供者が意図しないサービスの停止が発生する可能性があります。

https://jprs.jp/tech/security/2016-10-21-bind9-vuln-malformed-options.html

CVE-2016-2848の内容

- 影響のあるバージョン
  - 9.9系列：9.9.0～9.9.3rc1
  - 上記以外の系列：9.1.0～9.8.5rc1
  - 「fix #3548」を適用していないもの
- ISCの公開している最新バージョンは影響なし
- 外部からDNSメッセージひとつで強制終了
- **"active exploit"**は見つかっていない

CVE-2016-2848の影響を受けるパッケージ

OS	Version	Affected ?
RedHat 5	9.3.6-25.P1.el5_11.9(bind9)	Affected
RedHat 5	9.7.0-21.P2.el5_11.7(bind97)	Affected
RedHat 6	9.8.2-0.47.rc1.el6_8.1	Affected
Ubuntu 12.04	9.8.1.dfsg.P1-4ubuntu0.17	Affected
Debian 7	9.8.4.dfsg.P1-6+nmu2+deb7u10	Affected
Amazon Linux	9.8.2-0.37.rc1.48.amzn1	Affected
Infoblox NIOS 6	6.12.19	Affected ? (*1)
BIG-IP	12.1.1など	Not Affected(*2)

(*1)10/21にアップデートがリリースされていることから推測(リリース内容は未確認)

(*2)最新のHotFixを適用済みならば影響なし

https://support.f5.com/kb/en-us/solutions/public/k/01/sol01471335.html

最後に

- 公開された脆弱性を検証することで、その対応の不備や新たな脆弱性を発見できる場合がある
  - PowerDNS Security Advisory 2015-01に続き2回目

    https://doc.powerdns.com/md/security/powerdns-advisory-2015-01/
- 脆弱性を発見した場合は、パブリックなメーリングリストやバグトラッカに投稿せずに、まずは各ベンダ・プロジェクト・IPAの手続きを参照
  - ISC: https://www.isc.org/downloads/software-support-policy/security-advisory/
  - RedHat: https://access.redhat.com/security/team/contact
  - Ubuntu: https://wiki.ubuntu.com/SecurityTeam/FAQ#Contact
  - Debian: https://www.debian.org/security/faq#discover
  - IPA: https://www.ipa.go.jp/security/vuln/report/#contact