OSS DNSサーバソフトウェア アップデート情報

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

BIND9

前回までの脆弱性のおさらい

	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“(緊急)”→◎ 無印→○
同日公開のものは1つにまとめてある

その後１年分の脆弱性

	1	2	3	4	5	6	7	8	9	10	11	12
2009							◎					
2010							◎					◎
2011		◎			○	◎	◎					○/◎
2012						◎	○		◎	◎		○
2013	○		◎			◎	◎					
2014	◎				◎	◎						○/◎
2015		○					◎/◎		◎			◎
2016	◎		◎				○		◎	◎	◎	
2017	◎	○		◎	△	◎						

脆弱性サマリ

- 脆弱性が発表された回数: 9回(月)/13月
- 脆弱性の件数: 15件 (うち ”緊急” 8件(6回))

脆弱性分析

- 無条件コロリ: 4回(6件)
- DNS64＆別の機能の組合せ: 2件
- 最近の追加機能で落ちる: 2件
- lwresd: 1件
  - 9.12で削除予定
- 脆弱性を修正したら、別の脆弱性: 1件
- Windows Installerで権限昇格: 1件

脆弱性分析

- 本家は平気だけど、distributionのpackageが影響を受ける: 2件
  - RHEL5,6, Ubuntu, Debianのみで影響
    - CVE-2016-2848 坂口さんが見つけた物
      - » 本家は過去のリリース時の修正で影響を受けなくなっていた
  - RHEL6のみで影響
    - CVE-2017-3139 DNSSEC validation有効のときに落ちる

脆弱性分析

- BINDコロリは未だ出尽くしていなかった
- .0は、やはり枯れていなくて危ない
  - 新機能追加→脆弱性のループ は継続
- 今のBIND9は開発者にも手に負えない
  - 9.12でrefactoringするための資金集め中
    - 次のESVは9.11ですが、そちらにはマージされませんよね…。
      - 9.11以下で潜んでいる脆弱性はそのまま
      - refactoringして、潜んでいた脆弱性が見つかる可能性

脆弱性分析

- 脆弱性の修正で別の脆弱性が混入
- 4月の脆弱性は、元々は3月中に出る予定だったが、修正が不十分だった OR 追加の脆弱性が見つかったかで、4月までリリースが遅れた模様
  - 9.9.9-P7, 9.10.4-P7, 9.11.0-P4が欠番になっている
  - gitのpushが30日以上止まっていた (最終的に57日)
  - shodanでP7, P4が一旦観測されていた

余談: P8は圧巻 (いままでの最高はP4まで)

new release

- BIND 9.11.0 (10/4)
  - 新機能沢山
    - Catalog zone, LMDB(*),DynDB, dnstap, dnsec-keymgr, SERVFAIL TTL, Negative Trust Anchor, EDNS Client Subnet(auth), EDNS EXPIRE, 新RR Type, minimal-any, fetch limit default ON

  *) ゾーンの動的な追加・削除で不具合あり (～9.11.1)

  ※ **次期ESV。**現ESVの9.9は2018/06まで
- BIND 9.9.10, 9.10.5, 9.11.1 (4/19)

BIND以外

脆弱性

- 無限AXFR/IXFR
  - DNS Summer day 2016で坂口さんが発表した物
  - 各権威DNSサーバ実装が影響を受けた
- PowerDNS
  - 細工されたクエリでCPU浪費
  - 細工したゾーン情報でinteger overflow

脆弱性

- TSIG鍵の検証不備
  - PowerDNS
  - KnotDNS

*these versions fix a flaw within the TSIG protocol implementation that would allow an attacker with **a valid key name and algorithm to bypass the TSIG authentication** if no additional ACL restrictions is set.*

2.5.2, 2.4.5リリースアナウンスより

新機能

- Unbound
  - view機能(!)
  - serve-expired
  - source IP rate limit
  - Response actions based on IP address
  - EDNS Client subnet

新機能

- PowerDNS Authoritative Server
  - ALIAS record, API, Dynamic DNS
- PowerDNS Recursor
  - RPZ, EDNS Client subnet

Ongoing Innovation

IIJ Internet Initiative Japan

Any Questions?