BINDの脆弱性が出る
タイミングを見抜く力を！

For BIND lovers.

Yutaka FUJIWARA

2016/12/01

DNSOPS.JP BOF

予報士の実力とやらを…

提供

見せてもらおうか…

予報士！

- ありがとうございます！

https://twitter.com/ttkzw/status/689645470700810241

でも実態は予想屋みたいな…

- 大井競馬場で予想屋が聴衆へ予想を披露している風景
出典:Wikipedelia - 予想屋 https://ja.wikipedia.org/wiki/予想屋

脆弱性が出るタイミングを知りたい！

- 「重複の足音」が聞こえていれば…
  - ✓他の作業との調整ができるよね
  - ✓作業者アサインの調整ができるよね
  - ✓余裕をもって作業ができるよね
    - 心理的にも時間的にも…

- そもそもBIND使わなければいいのでは?
  - ✓確かに！ でも「そもそも論」はまた後ほど…

BINDの脆弱性、公開までの流れ

Xデーまでに起こるイベント(の勝手な推測)

- X-28Day　：脆弱性発覚、対応開始
- X-?　：ASN展開
- X-5bizDay　：修正版先行配布
- X-0Day　：Public Disclose

この辺の兆候が掴めると、なんとなく予報できそうな気がする！

X-28Day　：脆弱性発覚、対応開始

X-?　：ASN展開

X-5bizDay　：修正版先行配布

X-0Day　：Public Disclose

情報収集についての基本的な考え方

- 公開情報の合法的な収集と分析(OSINT)
  - 収集→分析→評価→仮説形成
  - Data→Information→Intelligence→Knowledge
    - ✓集めた情報に意味を持たせ、仮説をたてる
    - ✓「データが無い(不存在)」ことも情報

公開情報

- ISC公式Webサイト
- ML(ISC, OARC)
- Twitter (@ISCdotORG)

この辺のソースだけで予報は正直厳しいので、他の公開情報を探る…

使えそうなネタとなるとこの辺…

a. Gitのcommit log

b. FTPの特定ディレクトリ

c. 世界各地のversion.bind

d. LinuxのdistributionのBTS

実際のところa, b だけでも何とかなる

c,dは「保険」
予測の補正のため

Commit log

https://source.isc.org/

- 脆弱性対応開始以降の更新が見えなくなる
- 更新停止から4〜5週間でPublic Disclose

止まるだけ止まって何も出ず…ということもある…

過去の事例

CVE#	suspend	disclose
2016-8864	10/20	11/2
2016-2776	9/7	9/28
2016-1286	2/11	3/10

FTPの特定ディレクトリ

ftp.isc.org/isc/bind9/private/

- パッチの先行配布に用いるディレクトリと推定
  - ✓子ディレクトリの名前を知らないとアクセス不可
- 先行配布の際にタイムスタンプが更新
- その数日(3〜5営業日)後にPublic Disclose

version.bind

- 修正版先行配布を検知できる場合がある
- ざっくりshodanで探す（更新が遅いのが難点）
  - 例: https://www.shodan.io/search?query=%229.10.4-P4%22+OR+%229.9.9-P4%22+OR+%229.9.9-S6%22+OR+%229.11.0-P1%22+port%3A%2253%22
- 出現の偏りで影響範囲(キャッシュのみか否か)が分かる場合もある
- なぜか北欧方面(.seとか.no)が出現早い傾向、理由不明

Linux 各distributionのBTS

- ISCから各Distへ事前通知が展開される
  - ALT Linux, Amazon Linux AMI, Arch Linux, Chrome OS, Debian, Gentoo, MontaVista Software, Openwall, Oracle, Red Hat, Slackware, SUSE, Ubuntu, Wind River
- 方々のBTSを眺めていると、たまに事前対応の様子が見えてしまう時がある…

この流れで仮説形成

X-28Day　：脆弱性対応開始　→ Git更新が止まる

X-?　：ASN展開

X-5bizDay　：修正版先行配布　→ タイムスタンプ更新

→ 新version.bind出現

→ 各distributionの対応

X-0Day　：Public Disclose　→ 重複出来！

まとめ

- ある程度の予測は可能
  - あくまでも仮説であり「目安」
  - いつも上手くいくとは限らない
  - 突然公開されるものもある
    - ✓攻撃コードが公開されている状況等
    - ✓これはしょうがない…

ところで…

- 今回紹介した手法
  - ✓しばらくはこの手法で観測できるかもしれない
  - ✓今後仕様変更等で見られなくなる可能性もある
  - ✓この話を耳にしたISCが、GitやFTP等の情報を秘匿する可能性もあるため、恒久的なものではない
  - ✓タイミングは見抜けるが、本質を見抜いているか?

見抜く

- この予報自体がバッドノウハウ
  - ✓自分でやっといてなんだけど…
  - ✓いつまでも通用する手法とは思えない
  - ✓ISC次第だったりもする

- 見抜くべきは?
  - ✓そもそもBINDを使わないということかと…

それでもBIND使います？

詳細は下記資料参照

http://dnsops.jp/event/20160624/BINDからの卒業_配布用.pdf

おわり

See you!