「重複をお許しください」ができるまで

2011年4月20日

DNSOPS.JP BoF

株式会社日本レジストリサービス
森下泰宏（Orange）

本日の内容

- 「重複をお許しください」とは…
  - 生い立ちと状況
  - なぜいつも同じ書き出しなのか？
  - 「重複をお許しください」の主な分類
- 「重複をお許しください」ができるまで
  - ケーススタディ
    - BIND 9の脆弱性
    - qmail/netqmailの512バイト問題
  - できるまでの流れ
  - 作るにあたり気を付けていること
  - 実例紹介

「重複をお許しください」とは…

- 技術コミュニティ系メーリングリストに私がマルチポストの形式で出す、「お知らせ」の書き出し
- 初出は2010年6月9日…だったようです
  - [janog:09571] と [DNSOPS dnsops 929]
  - 「DNSSECの円滑導入と安定運用の実現のために - 考えなければならない「対応と現実」」 - 公開のお知らせ
- 2011年4月19日までの間に合計24通をMLに送信
  - およそ2週間に1通程度の割合
  - DNSSEC関連のアナウンス：15通
  - BIND 9の脆弱性についての注意喚起：5通

「重複をお許しください」の状況

- なぜいつも同じ書き出しなのか？
  - そもそもは過去のメールの再利用→自然と同じ書き出しに
- Internet Week 2010の会場にて…
  - 「重複をお許しください」をMLで見ると緊張が走る
  - 「仕事が増えるフラグ」
    - でも、私が増やしているわけではないはずです
- twitterにおける最近の反応から

「重複をお許しください」の主な分類

今日の話題はこれ

DNSに関連する..

- セキュリティホールや不具合などに関する注意喚起
  - BIND 9の脆弱性情報
  - qmail/netqmailの512バイト問題
- インターネット全体に影響がある情報のアナウンス
  - ルートゾーンで.jpのDSが公開
  - .comのDS公開にあたり、ISCがアドバイザリを公開
- 技術文書公開のお知らせ
  - JP DPSの公開
  - DNSSEC関連RFCの翻訳の公開

ケーススタディ：BIND 9の脆弱性

- ISCからの「Advance Security Notification（ASN）」が重要な情報源
  - セキュリティアドバイザリを先行して通知
  - BIND and DNS support services の一環
    詳細はhttps://www.isc.org/services/support/bindを参照
  - JPRSはBIND Forumメンバー（Premium Service）
  - 一般へのアナウンスはASNから一定期間経過後
- ただし、2009年7月のDynamic Updateに関する実装上の脆弱性（通称：BINDコロリ）では、ASNから間をおかずに一般にもアナウンスされた
  - 既にExploitコードが広く公開されていたため

①ASNのラフ分析、行動是非の判断

1) ASNを分析（1）
   - 重要な3つの要素
     - 危険度（Severity:、Exploitable:）
     - 対象（Versions affected:）
     - 既にExploitがあるか（Active exploits:）
2) 出すかどうかを判断
   - 上記情報により「重複をお許しください」を出すべきかどうかを判断する
   - 「Severity: High」「Exploitable: remotely」となっていた場合、（私の）気分がブルーになる

②ASNの詳細分析、文案作成

3) ASNを分析（2）
- 詳細を分析する
  - 何の不具合か（実装上、プロトコル上、構造上、etc.）
  - できてしまうことは何か（BINDを落とせる、本来入れられない嘘の応答を入れられる、DNSSEC検証をパスできる、etc.）
  - 何をすればよいのか（Workarounds:、Solution:）

4) 文章の素案を作成
- タイトルを決める
  - 「（緊急）」の有無、推奨度「～を（強く）推奨」など
- 構成を決める
  - 基本的にはテンプレートで
  - 「概要」「詳細」「対策」「オリジナル情報へのリンク」
  - 必要に応じ項目を適宜追加（「背景」など）

③文書作成とレビュー、追試

5) 文章の中身を作成
  - 文書の作成とレビュー
    - テクニカルレビュー（書いてあることが正しいか）
    - 広報的レビュー（わかりやすいか、誤解を生まないか）

6) 動作の確認（追試）
  - 書いてあることが実際に起こるかどうか
    - 重要な事項（かつてのBINDコロリなど）では特に注意して実施

- 実際には3)～6)は並列的に実施される

④アナウンス、アフターフォロー

7) アナウンス
- ISCのWebを定期的にチェックし、文書の公開を確認
  - CVEやCERTのWebについても適宜確認
- JPRS Webの更新
- MLへの送信(「重複をお許しください」)

8) アフターフォロー
- 情報の広まり具合と対応状況のチェック
  - 重要な2つのメディア:twitter、セキュリティホールmemo
  - 検索エンジンの状況(掲載状況、検索順位の変化など)
  - 各種ブログやメディア等における掲載状況
  - 各サイトにおける対応状況
- 問い合わせ対応

作るにあたり気を付けていること

- 「概要」を読むだけで以下のことがわかるようにする
  - 対象、何の不具合か、どういうことができてしまうのか、情報源、危険性、どうする必要があるのか
- 「対策」には、必要な対策について簡潔に記述する
  - かつ、一時的回避策と根本的解決策を明確に区別する
- 「詳細」は、興味を持った人が技術的詳細や実際にできることの詳細を知りたいために読む場所にする
  - 詳細を読まなくても、必要な対応ができるようにする
  - 例外条件（この場合は影響なし）がある場合、ここに記述
- 情報源や必要なパッチへのリンクを掲載する
  - 情報のソースと必要な情報に到達できるようにする

実例：2011年2月23日発表

- 【概要】9.7.2-P2以前のBIND 9には、DNSSEC署名された否定応答を受信した際のキャッシュ済みRRSIGレコードの取り扱いに不具合があり、リモートからのサービス不能（DoS）攻撃が可能になる脆弱性が存在することが、開発元のISCより発表されました。本脆弱性は危険度が高いため、該当するBIND 9を利用しているユーザは、関連情報の収集や緊急パッチの適用等、適切な対応を取ることを強く推奨します。

実例：2011年2月[illegible]発表

- 【概要】9.7.2-P2以前のBIN[illegible] DNSSEC署名された否定応答を受信した際のキャ[illegible] RRSIGレコードの取り扱[illegible]かねないキャッシュトからのサ[illegible]不能（DoS）攻撃が可能になる脆弱性が存在することが、開発元のISCより発表されました。本脆弱性は危険度が高いため、該当するBIND 9を利用しているユーザは、関連情報の収集や緊急パッチの適用等、適切な対応を取ることを強く推奨します。

対象

何の
不具合か

どういうことが
できてしまうのか

情報源

危険性

どうする
必要があるのか

ケーススタディ：qmailの512バイト問題

- 基本的な考え方はBIND 9の脆弱性の例と同じ
- 開発元の公式発表を受けたものではないため「どこが発表したのか（情報源）」の項目がない
  - 「JPRSが発表した」ということになる
- そのため「問題の概要」の前に「背景」を記載
  - 問題の概要について説明する前に、「どのような動作が技術的に正しくかつ望ましいのか」を明確にしておく必要があるため
  - 技術的な背景と望ましい動作について記述
    - あくまで技術的・中立的に記述
    - 仕様や望ましい動作について記述する場合、その根拠を明確に

実例：2011年3月3日発表

- 【背景】…そのうち、TCPの使用は従来からあるDNSの基本機能の一つであり、インターネットに接続するホストが満たすべき要件を定めたRFC 1123では、DNSにおけるTCPの使用を「サポートすべき（SHOULD support）」と定めています。そして、TCPを使用することでDNSでは65,535バイトまでのDNS応答を取り扱うことができ、これがDNSの仕様においてサポートされるDNS応答の最大サイズとなります。

  ただし、DNSの仕様では負荷軽減の観点から、通信時にはUDPを最初に使用し、TCPの使用は応答の大きさが512バイトを超え、応答パケットの切り詰めが発生した場合のみとすることを定めています。そのため、DNS応答の大きさが512バイトを超えない場合、ゾーン転送以外の通常のDNS運用でTCPが使用されることはありません。

実例：2011年3月3日発表

- 【背景】…そのうち、TCPの使[illegible]あるDNSの基本機能の一つであり、インターネットに接続するホ[illegible]べき要件を定めたRFC 1123では、DNSにおけ[illegible]support）」と定[illegible]DNSでは65,535バイトまでのDNS応答を取り扱うことができ、これがDNSの仕様においてサポートされるDNS応答の最大サイズとなります。

根拠①-1

根拠①-2
（RFC 1035
4.2.2. TCP usage）

根拠を明確に示してなかった！
（減点1）

事実①

根拠②

[illegible]、DNSの仕様では負荷軽減の観点から、通信時にはUDPを最初に使用し、TCPの使用は応答の大きさが512バイトを超え、応答パケットの切り詰めが発生した場合のみとすることを定めています。そのため、DNS応答の大きさが512バイトを超えない場合、ゾーン転送以外の通常のDNS運用でTCPが使用されることはありません。

事実②

最後に…まとめのようなもの

- 今後も必要に応じてできるだけ迅速に「重複をお許しください」を出す予定です
  - お騒がせいたしますが、よろしくお願いします
- 文書作成技術や広報技術に関するさまざまなノウハウを、蓄積・共有していければいいなと思っています
- 繰り返しますが、私が仕事を増やしてるわけではないはずです
  - メールが来ても不機嫌にならないでください
  - たんたんと必要な対応をお願いいたします
- でも、朝会社に来た時に「げげ、まじかよ…」となるメールは、やっぱりつらいのかも…
  - ISCからの不幸のメールを受け取った時の私を思うと…

やはり私も不幸のメールを出しているのかもしれません…

おまけ：qmailの件がなぜいまいちなのか

6つの「まずいところ」

1. 送り側が何年も設定を変えてないのにおかしくなる
   ⇒送れないのは自分のせいだという認識が薄い
2. 受け側がDNSSECを入れた所だけがおかしくなる
   ⇒やっぱり相手が設定を間違えたに違いないと思われる
3. いわゆる「簡単パッケージ」に組み込まれている場合がある
   ⇒そもそも自分がqmailのユーザーだとは思っていない
4. SMTPセッションが張られる前にこける
   ⇒受け側でエラーが起こっていることがわからない
5. エラーメッセージからは真の原因がわかりにくい
   ⇒deferral: CNAME_lookup_failed_temporarily._(#4.4.3)
6. デフォルトでは1週間後に初めてエラーメールが戻る
   ⇒受け側でのDNSSEC導入後、しばらくは発覚しない

Q and A