

JPRSの技術情報発信 (2024年7月～2025年6月)

2025年6月27日

DNS Summer Day 2025

株式会社日本レジストリサービス (JPRS)

森下 泰宏

本日より紹介する技術情報発信

1. 脆弱性情報

- BIND
- BIND以外のDNSソフトウェア

2. DNS運用に関する技術情報

- サブドメインテイクオーバー・NSテイクオーバーに関する情報発信
- JPRSが情報提供の対象とするBIND 9のバージョンについて

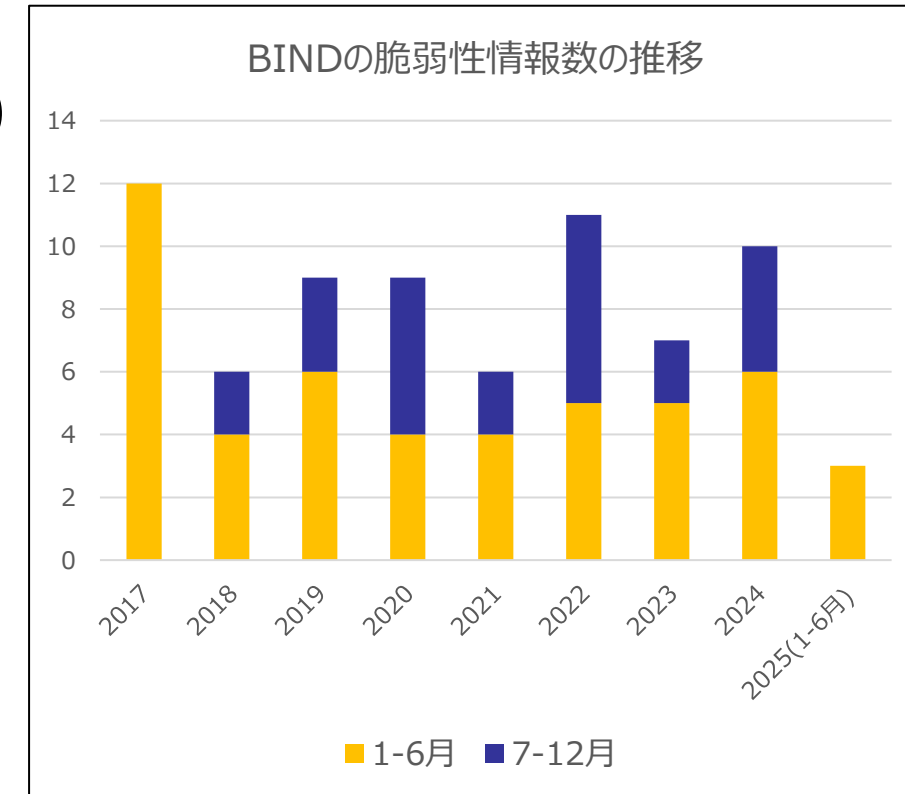
JPRSが公開した脆弱性情報

- **BIND（7件（緊急7件））**

- 2024年7月～12月：4件（前年同期：2件）
- 2025年1月～6月：3件（前年同期：6件）

- **BIND以外（7件）**

- Knot Resolver（1件）
- PowerDNS Recursor（2件）
- Unbound（1件）
- Windows DNS（3件）



（カッコ内はJPRSが発信した脆弱性情報の件数）

脆弱性情報（BIND） [1/2]

公開日	タイトル・URL	概要
2024/7/24	（緊急） BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2024-4076） < https://jprs.jp/tech/security/2024-07-24-bind9-vuln-serve-stale.html >	serve-staleの実装不具合 serve-stale使用時のみ
2024/7/24	（緊急） BIND 9.xの脆弱性（過剰なCPU負荷の誘発）について（CVE-2024-1975） < https://jprs.jp/tech/security/2024-07-24-bind9-vuln-sig0.html >	sig(0)の実装不具合
2024/7/24	（緊急） BIND 9.xの脆弱性（パフォーマンスの低下）について（CVE-2024-0760） < https://jprs.jp/tech/security/2024-07-24-bind9-vuln-dnsmessage.html >	多数のDNSメッセージを TCPで送りつけると パフォーマンスが低下 ※影響大
2024/7/24	（緊急） BIND 9.xの脆弱性（パフォーマンスの低下）について（CVE-2024-1737） < https://jprs.jp/tech/security/2024-07-24-bind9-vuln-resourcerecords.html >	同じドメイン名に大量の RRを設定したデータを 保持・キャッシュすると パフォーマンスが低下 ※影響大

多数・大量の〇〇でパフォーマンスが低下する脆弱性が2件公開

CVE-2024-0760

- 多数のDNSメッセージをTCPで送りつけるとパフォーマンスが低下
- 攻撃方法が単純、かつ影響が大きい
 - フルリゾルバーと権威DNSサーバーの双方が対象
 - リモートからの問い合わせのみで脆弱性をトリガー可能
 - namedの設定・オプションやACLでは影響を回避・軽減できない

もし未対応だった場合、すぐに対応が必要

CVE-2024-1737

- 大量のRRを設定したデータを保持・キャッシュするとパフォーマンスが低下
- 報告者：坂口俊文氏
- 本脆弱性により、BINDのRRの最大数が100に制限
 - max-records-per-typeオプションとmax-types-per-nameオプションが追加（デフォルト値はいずれも100）

RRset limits in zones
<<https://kb.isc.org/docs/rrset-limits-in-zones>>



Toshifumi Sakaguchi
@siskrn

再掲&本命:デカデカRRSetsを用意するだけの簡単なお仕事。



Yasuhiro Morishita @OrangeMorishita · 2024年7月24日
権威サーバー「いいから食べ」

2



86



Toshifumi Sakaguchi
@siskrn

これからのBINDはお口が小さくなりましたね。

脆弱性情報 (BIND) [2/2]

公開日	タイトル・URL	概要
2025/1/30	(緊急) BIND 9.xの脆弱性 (パフォーマンスの低下) について (CVE-2024-12705) < https://jprs.jp/tech/security/2025-01-30-bind9-vuln-dnsoverhttps.html >	DNS over HTTPSの実装不具合
2025/1/30	(緊急) BIND 9.xの脆弱性 (過剰なCPU負荷の誘発) について (CVE-2024-11187) < https://jprs.jp/tech/security/2025-01-30-bind9-vuln-additionalsection.html >	Additionalセクションに多数のRRを含む応答を生成・処理するとパフォーマンスが低下
2025/5/22	(緊急) BIND 9.20.xの脆弱性 (DNSサービスの停止) について (CVE-2025-40775) < https://jprs.jp/tech/security/2025-05-22-bind9-vuln-tsig.html >	TSIGの実装不具合 TSIGを使っていない場合も対象 ※影響大、ただしBIND 9.20.xのみ

多数・大量の〇〇でパフォーマンスが低下する脆弱性が**また公開**

TSIGは古くからある機能なのに**BIND 9.20.xのみ**？

CVE-2024-11187

- **Additionalセクションに多数のRRを含む応答を生成・処理するとパフォーマンスが低下**
 - Additionalセクションにはグルーレコードや、MXレコードで指定されたメールサーバーのIPアドレス（返せる場合）などが返る
- **報告者：坂口俊文氏**



CVE-2025-40775

- 以下の3条件（**BINDコリ級**）をすべて満たしている
 - フルリゾルバーと権威DNSサーバーの双方が対象
 - リモートからのパケット一つでnamedがダウン
 - namedの設定・オプションやACLでは影響を回避・軽減できない
- ただし、**BIND 9.20.xのみ**
 - 9.19.xで行われた**TSIG**のコードのリファクタリングで、今回のバグが混入
 - 9.18以前の系列は**対象外**

脆弱性情報（BIND以外） [1/2]

公開日	タイトル・URL	概要
2024/8/16	Windows DNSの脆弱性情報が公開されました（CVE-2024-37968） < https://jprs.jp/tech/security/2024-08-16-windowsdns.html >	実装不具合によりDNS スプーフィングが可能
2024/10/7	PowerDNS Recursorの脆弱性情報が公開されました（CVE-2024-25590） < https://jprs.jp/tech/security/2024-10-07-powerdns-recursor.html >	特別に細工された 応答を繰り返しキャッ シュするとパフォーマ ンスが低下
2024/10/7	Unboundの脆弱性情報が公開されました（CVE-2024-8508） < https://jprs.jp/tech/security/2024-10-07-unbound.html >	ドメイン名圧縮・展開を 伴う非常に大きな RRsetを処理すると パフォーマンスが低下
2024/11/15	Windows DNSの脆弱性情報が公開されました（CVE-2024-43450） < https://jprs.jp/tech/security/2024-11-15-windowsdns.html >	実装不具合によりDNS スプーフィングが可能

多数・大量の〇〇でパフォーマンスが低下する脆弱性が**ここでも公開**

CVE-2024-25590 ・ CVE-2024-8508

- CVE-2024-25590 (PowerDNS Recursor)
 - 特別に細工された応答を繰り返しキャッシュするとパフォーマンスが低下
- CVE-2024-8508 (Unbound)
 - ドメイン名圧縮・展開を伴う非常に大きなRRsetを処理するとパフォーマンスが低下
- 報告者：いずれも坂口俊文氏



脆弱性情報（BIND以外） [2/2]

公開日	タイトル・URL	概要
2025/3/17	Windowsドメインネームサービスの脆弱性情報が公開されました（CVE-2025-24064） < https://jprs.jp/tech/security/2025-03-17-windows.html >	RCE脆弱性 ※影響大
2025/4/10	PowerDNS Recursorの脆弱性情報が公開されました（CVE-2025-30195） < https://jprs.jp/tech/security/2025-04-10-powerdns-recursor.html >	特定のRRSetを含む 応答を処理・キャッシュ するとサーバープロセス がクラッシュ
2025/4/28	Knot Resolverの脆弱性情報が公開されました < https://jprs.jp/tech/security/2025-04-28-knotresolver.html >	特定の条件下での 予期しないサーバーの クラッシュを回避

• CVE-2025-24064（RCE脆弱性）

- すべてのWindows Serverが対象、CVSS値が8.1と高いので要注意
- Microsoftは「**緊急**」と評価

サブドメインテイクオーバー・ NSテイクオーバーに関する情報発信

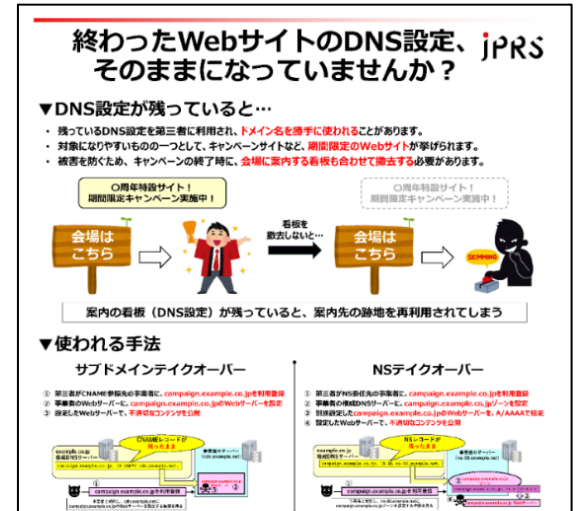
● 注意喚起・パンフレットの公開

サービス終了後に残っているDNS設定を利用したサブドメインの乗っ取りについて
[＜https://jprs.jp/tech/security/2025-01-21-danglingrecords.html＞](https://jprs.jp/tech/security/2025-01-21-danglingrecords.html)

終わったWebサイトのDNS設定、そのままになっていませんか？ (PDF)
[＜https://jprs.jp/tech/security/2025-01-21-danglingrecords.pdf＞](https://jprs.jp/tech/security/2025-01-21-danglingrecords.pdf)

● イベント・カンファレンスでの情報発信

- JANOG55 (2025年1月)
- APAN 59 (2025年3月)
- Interop Tokyo 2025 (2025年6月)



JPRSが情報提供の対象とする BIND 9のバージョンについて

- **2025年5月26日公開**

JPRSが情報提供の対象とするBIND 9のバージョンについて
<<https://jprs.jp/tech/security/2025-05-26-bind9-version.html>>

- **JPRSが情報提供の対象とするBINDのバージョンを明確化**

- ISCが一般公開し、かつ、本番環境での使用を想定した、**安定バージョン**と**拡張サポートバージョン**の2種類が対象

BINDのバージョンによる分類とは？

参考：BINDのバージョンによる分類（ISC）

分類	説明	例
開発バージョン (Development versions)	メジャーバージョンが奇数のもの。 新機能や大幅なリファクタリングが含まれ、 新機能の実験・フィードバック のためにリリースされる。	9.19.x 9.21.x
安定バージョン (Stable versions)	メジャーバージョンが偶数のもの。 本番環境を想定した安定版としてリリースされる。 なお、ISCでは大規模な本番環境への導入は 3回目のメンテナンスリリース まで待つことを推奨している。	9.18.x 9.20.x
拡張サポートバージョン (Extended Support versions)	ESVと略され、 安定性を重視するバージョン として、 安定バージョンから選ばれる。サポート期間が延長され、 最初のリリースから4年間のサポートが保証 される。	9.18.x
サポートプレビュー (Supported Preview)	ISCの有償サポート顧客を対象 とした、開発中の新機能 の早期アクセスを含むバージョン。一般公開されず、 -S という特別なサフィックスが付けられる。	9.18.26 -S1

**JPRSの
情報提供
対象**

ISC's Software Support Policy and Version Numbering
<<https://kb.isc.org/docs/aa-00896>>

**JPRSでは今後もさまざまな形で
技術情報発信を続けていきます！**



<<https://jprs.jp/tech/>>



@JPRS_official



JPRSofficial



JPRSpress