Domain Name System Operations   Z. Li
Internet-Draft   W. Wu
Intended status: Standards Track   Chinese Academy of Sciences
Expires: 27 June 2026   J. Yan
                              China Internet Network Information Center
                                                                  Z. Li
                                            Chinese Academy of Sciences
                                                                 Z. Yan
                              China Internet Network Information Center
                                                      24 December 2025

Minimizing ANY-Query Responses at Recursive Resolvers
draft-li-any-responses-minimization-00

Abstract

The " ANY " query type in DNS requests the server to return all available resource records for a given domain name. While RFC 8482 defines a mechanism for authoritative servers to minimize ANY responses, a recursive resolver may still generate an ANY query response directly from its cache, thereby bypassing the authoritative side’s ANY query minimization strategy. This document provides supplementary guidance for recursive resolvers on processing ANY queries to mitigate potential operational and security issues.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 27 June 2026.

Copyright Notice

Table of Contents

1. Introduction

The Domain Name System (DNS) specifies a query type known as the "ANY "query (QTYPE=255). In operational deployments, the handling of ANY queries may raise both operational and security considerations. [RFC8482] defines a mechanism for authoritative servers to provide minimized responses to ANY queries; however, recursive resolvers may generate ANY responses directly from cached resource record sets (RRsets), thereby bypassing the minimization performed by authoritative servers. As a result, authoritative-side minimization alone does not fully mitigate the security risks posed by ANY queries. This document supplements existing mechanisms by providing guidance on response-minimization strategies for recursive resolvers when processing ANY queries.

1.1. Terminology

This document uses terminology specific to the Domain Name System (DNS), descriptions of which can be found in [RFC8499].

This document uses the term "ANY query" for DNS meta-queries that specify QTYPE=ANY, and uses "ANY response" for the DNS responses produced in that context.

1.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Motivation

ANY queries raise various operational and security considerations in practical deployments. This section first outlines these issues and then identifies why reliance solely upon the authoritative-side minimization mechanism defined in [RFC8482] is insufficient to fully mitigate these risks.

2.1. Operational and Security Issues Associated with ANY Queries

ANY queries may cause a server to return multiple records beyond what the client actually requested, thereby increasing the risk of information disclosure. This naturally leads operators toward minimizing such responses.

Responses to ANY queries are often large in size and can be abused in DNS-based amplification attacks. An attacker can spoof the source IP address and send ANY queries to resolvers, causing large responses to be reflected to a victim, thereby amplifying the attack (see [RFC5358]).

Processing an ANY query requires the DNS server to aggregate multiple resource records to generate a response, and these responses are typically large, which can introduce additional operational burden.

ANY responses are frequently large enough to cause IP datagram fragmentation. Fragmentation during transmission or handling can introduce additional security risks, including packet loss and blocking.

Different DNS servers may adopt inconsistent methods for processing ANY queries or generating response content, resulting in unpredictable behavior. This unpredictability may lead to operational challenges and could potentially be exploited to create security risks.

2.2. Limitations of Authoritative-Side Minimization

Although [RFC8482] defines a mechanism for authoritative servers to minimize responses to ANY queries, recursive resolvers may generate ANY responses directly from cached RRsets (e.g., A, AAAA, TXT records) without retrieving minimized results from authoritative servers. As a result, the ANY responses returned by recursive resolvers to clients can still be large, potentially leading to information disclosure, amplification attacks, and other operational and security issues. Therefore, relying solely on authoritative-side minimization is insufficient to fully mitigate these risks. This document provides complementary guidance for recursive resolvers on minimizing responses to ANY queries in order to reduce the potential impact.

3. Handling of ANY Queries by Recursive Resolvers

3.1. Overview

To mitigate the operational and security risks associated with ANY queries, this section first defines the core defensive principle for recursive resolvers: a resolver SHOULD rely on the authoritative server’s minimized response as the basis for answering ANY queries and SHOULD avoid constructing an ANY response that exceeds the size of the authoritative response by synthesizing data from its local cache.

In addition, recognizing that some authoritative servers have not yet deployed response minimization for ANY queries, a recursive resolver MAY implement supplementary mitigation measures in accordance with its local policy and operational requirements.

3.2. Core Defense Mechanism

A recursive resolver can maintain a dedicated cache for ANY queries to avoid combining multiple cached RRsets into an excessively large ANY response, which helps reduce potential security risks. In this case, if the authoritative server has deployed an ANY-query minimization mechanism, the recursive resolver SHOULD return the minimized response from the authoritative server directly to the client, rather than relying on locally cached RRsets to synthesize a larger ANY response.

In addition, since some authoritative servers may refuse or not support ANY queries, a resolver may consider applying negative caching for such responses.

3.3. Additional Mitigations

RRset Minimization and Response Byte Limits: A resolver MAY respond using a single RRset or a subset of available RRsets. However, certain RRsets (e.g., large TXT or RRSIG records) can have considerable size, and implementers SHOULD consider placing an upper bound on the total response size, such as limiting UDP responses to 512 bytes, to mitigate security risks.

Rate Limiting for ANY queries: A recursive resolver may apply a rate-limiting mechanism for QTYPE=ANY queries to reduce the risk associated with potential abuse. Since ANY queries may generate large response sizes, applying moderate rate limits can help mitigate potential risks. The specific rate-limiting policy is left to the implementer to determine based on local deployment considerations.

4. Implementation Experience

NSD implements a subset-mode response to ANY queries.

Unbound supports a "deny-any" mode, in which ANY queries are rejected.

BIND9 implements a single RRset response to ANY queries.

5. Security Considerations

[RFC8482] defines response-minimization mechanisms for authoritative servers, but these mechanisms do not constrain how recursive resolvers may synthesize large ANY responses from their caches. Such synthesized responses can still be exploited for reflection or amplification attacks.

This document provides complementary guidance for recursive resolvers to reduce the associated attack surface while preserving the availability of legitimate queries.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

6.2. Informative References

[RFC5358] Damas, J. and F. Neves, "Preventing Use of Recursive Nameservers in Reflector Attacks", BCP 140, RFC 5358, DOI 10.17487/RFC5358, October 2008, <https://www.rfc-editor.org/rfc/rfc5358>.

[RFC8482] Abley, J., Gudmundsson, O., Majkowski, M., and E. Hunt, "Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY", RFC 8482, DOI 10.17487/RFC8482, January 2019, <https://www.rfc-editor.org/rfc/rfc8482>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/rfc/rfc8499>.

Authors' Addresses

Zihan Li
Chinese Academy of Sciences
Beijing
China
Email: lizihan24z@ict.ac.cn

Wenhao Wu
Chinese Academy of Sciences
Beijing
China
Email: wuwenhao22s@ict.ac.cn

Jin Yan
China Internet Network Information Center
Beijing
China
Email: yanjin@cnnic.cn

Zhenyu Li
Chinese Academy of Sciences
Beijing
China
Email: zyli@ict.ac.cn

Zhiwei Yan
China Internet Network Information Center
Beijing
China
Email: yanzhiwei@cnnic.cn