Internet Engineering Task Force (IETF)
Request for Comments: 9567
Category: Standards Track
ISSN: 2070-1721

R. Arends
M. Larson
ICANN

April 2024

DNS Error Reporting

Abstract

DNS error reporting is a lightweight reporting mechanism that provides the operator of an authoritative server with reports on DNS resource records that fail to resolve or validate. A domain owner or DNS hosting organization can use these reports to improve domain hosting. The reports are based on extended DNS errors as described in RFC 8914.

When a domain name fails to resolve or validate due to a misconfiguration or an attack, the operator of the authoritative server may be unaware of this. To mitigate this lack of feedback, this document describes a method for a validating resolver to automatically signal an error to a monitoring agent specified by the authoritative server. The error is encoded in the QNAME; thus, the very act of sending the query is to report the error.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9567.

Table of Contents

1. Introduction

When an authoritative server serves a stale DNSSEC-signed zone, the cryptographic signatures over the resource record sets (RRsets) may have lapsed. A validating resolver will fail to validate these resource records.

Similarly, when there is a mismatch between the Delegation Signer (DS) records at a parent zone and the key signing key at the child zone, a validating resolver will fail to authenticate records in the child zone.

These are two of several failure scenarios that may go unnoticed for some time by the operator of a zone.

Today, there is no direct relationship between operators of validating resolvers and authoritative servers. Outages are often noticed indirectly by end users and reported via email or social media (if reported at all).

When records fail to validate, there is no facility to report this failure in an automated way. If there is any indication that an error or warning has happened, it may be buried in log files of the resolver or not logged at all.

This document describes a method that can be used by validating resolvers to report DNSSEC validation errors in an automated way.

It allows an authoritative server to announce a monitoring agent to which validating resolvers can report issues if those resolvers are configured to do so.

The burden to report a failure falls on the validating resolver. It is important that the effort needed to report failure is low, with minimal impact to its main functions. To accomplish this goal, the DNS itself is utilized to report the error.

2. Requirements Notation

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.

3. Terminology

This document uses DNS terminology defined in BCP 219 [RFC9499]. This document also defines and uses the following terms:

Reporting resolver: A validating resolver that supports DNS error reporting.

Report query: The DNS query used to report an error. A report query is for a DNS TXT resource record type. The content of the error report is encoded in the QNAME of a DNS request to the monitoring agent.

Monitoring agent: An authoritative server that receives and responds to report queries. This facility is indicated by a domain name, referred to as the "agent domain".

Agent domain: A domain name that is returned in the EDNS0 Report-Channel option and indicates where DNS resolvers can send error reports.

4. Overview

An authoritative server indicates support for DNS error reporting by including an EDNS0 Report-Channel option with OPTION-CODE 18 and the agent domain in the response. The agent domain is a fully qualified, uncompressed domain name in DNS wire format. The authoritative server MUST NOT include this option in the response if the configured agent domain is empty or is the null label (which would indicate the DNS root).

The authoritative server includes the EDNS0 Report-Channel option unsolicited. That is, the option is included in a response despite the EDNS0 Report-Channel option being absent in the request.

If the authoritative server has indicated support for DNS error reporting and there is an issue that can be reported via extended DNS errors, the reporting resolver encodes the error report in the QNAME of the report query. The reporting resolver builds this QNAME by concatenating the "_er" label, the QTYPE, the QNAME that resulted in failure, the extended DNS error code (as described in [RFC8914]), the label "_er" again, and the agent domain. See the example in Section 4.1 and the specification in Section 6.1.1. Note that a regular RCODE is not included because the RCODE is not relevant to the extended DNS error code.

The resulting report query is sent as a standard DNS query for a TXT DNS resource record type by the reporting resolver.

The report query will ultimately arrive at the monitoring agent. A response is returned by the monitoring agent, which in turn can be cached by the reporting resolver. This caching is essential. It dampens the number of report queries sent by a reporting resolver for the same problem (that is, with caching, one report query per TTL is sent). However, certain optimizations, such as those described in [RFC8020] and [RFC8198], may reduce the number of error report queries as well.

This document gives no guidance on the content of the RDATA in the TXT resource record.

4.1. Example

A query for "broken.test.", type A, is sent by a reporting resolver.

The domain "test." is hosted on a set of authoritative servers. One of these authoritative servers serves a stale version of the "test." zone. This authoritative server has an agent domain configured as "a01.agent-domain.example.".

The authoritative server with the stale "test." zone receives the

request for "broken.test.". It returns a response that includes the EDNS0 Report-Channel option with the domain name "a01.agent-domain.example.".

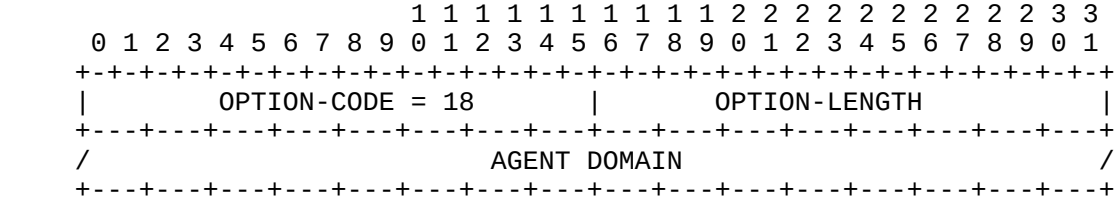
The reporting resolver is unable to validate the "broken.test." RRset for type A (an RR type with value 1), due to an RRSIG record with an expired signature.

The reporting resolver constructs the QNAME "_er.1.broken.test.7._er.a01.agent-domain.example." and resolves it. This QNAME indicates extended DNS error 7 occurred while trying to validate "broken.test." for a type A (an RR type with value 1) record.

When this query is received at the monitoring agent (the operators of the authoritative server for "a01.agent-domain.example."), the agent can determine the "test." zone contained an expired signature record (extended DNS error 7) for type A for the domain name "broken.test.". The monitoring agent can contact the operators of "test." to fix the issue.

5. EDNS0 Option Specification

This method uses an EDNS0 [RFC6891] option to indicate the agent domain in DNS responses. The option is structured as follows:



Field definition details:

OPTION-CODE: 2 octets; an EDNS0 code that is used in an EDNS0 option to indicate support for error reporting. The name for this EDNS0 option code is Report-Channel.

OPTION-LENGTH: 2 octets; contains the length of the AGENT DOMAIN field in octets.

AGENT DOMAIN: A fully qualified domain name [RFC9499] in uncompressed DNS wire format.

6. DNS Error Reporting Specification

The various errors that a reporting resolver may encounter are listed in [RFC8914]. Note that not all listed errors may be supported by the reporting resolver. This document does not specify what is or is not an error.

The DNS class is not specified in the error report.

6.1. Reporting Resolver Specification

Care should be taken when additional DNS resolution is needed to resolve the QNAME that contains the error report. This resolution itself could trigger another error report to be created. A maximum expense or depth limit MUST be used to prevent cascading errors.

The EDNS0 Report-Channel option MUST NOT be included in queries.

The reporting resolver MUST NOT use DNS error reporting if the authoritative server returned an empty AGENT DOMAIN field in the

EDNS0 Report-Channel option.

For the monitoring agent to gain more confidence that the report is not spoofed, the reporting resolver SHOULD send error reports over TCP [RFC7766] or other connection-oriented protocols or SHOULD use DNS Cookies [RFC7873]. This makes it harder to falsify the source address.

A reporting resolver MUST validate responses received from the monitoring agent. There is no special treatment for responses to error-reporting queries. Section 9 ("Security Considerations") contains the rationale behind this.

6.1.1. Constructing the Report Query

The QNAME for the report query is constructed by concatenating the following elements:

* A label containing the string "_er".
* The QTYPE that was used in the query that resulted in the extended DNS error, presented as a decimal value, in a single DNS label. If additional QTYPEs were present in the query, such as described in [MULTI-QTYPES], they are represented as unique, ordered decimal values separated by a hyphen. As an example, if both QTYPE A and AAAA were present in the query, they are presented as the label "1-28".
* The list of non-null labels representing the query name that is the subject of the DNS error report.
* The extended DNS error code, presented as a decimal value, in a single DNS label.
* A label containing the string "_er".
* The agent domain. The agent domain as received in the EDNS0 Report-Channel option set by the authoritative server.

If the QNAME of the report query exceeds 255 octets, it MUST NOT be sent.

The "_er" labels allow the monitoring agent to differentiate between the agent domain and the faulty query name. When the specified agent domain is empty, or is a null label (despite being not allowed in this specification), the report query will have "_er" as a top-level domain, and not the top-level domain from the query name that was the subject of this error report. The purpose of the first "_er" label is to indicate that a complete report query has been received instead of a shorter report query due to query minimization.

6.2. Authoritative Server Specification

The authoritative server MUST NOT include more than one EDNS0 Report-Channel option in a response.

The authoritative server includes the EDNS0 Report-Channel option unsolicited in responses. There is no requirement that the EDNS0 Report-Channel option be present in queries.

6.3. Monitoring Agent Specification

It is RECOMMENDED that the authoritative server for the agent domain reply with a positive response (i.e., not with NODATA or NXDOMAIN) containing a TXT record.

The monitoring agent SHOULD respond to queries received over UDP that have no DNS Cookie set with a response that has the truncation bit (TC bit) set to challenge the resolver to requery over TCP.

7. IANA Considerations

IANA has assigned the following in the "DNS EDNS0 Option Codes (OPT)" registry:

Value	Name	Status	Reference
18	Report-Channel	Standard	RFC 9567

Table 1

IANA has assigned the following in the "Underscored and Globally Scoped DNS Node Names" registry:

RR Type	_NODE NAME	Reference
TXT	_er	RFC 9567

Table 2

8. Operational Considerations

8.1. Choosing an Agent Domain

It is RECOMMENDED that the agent domain be kept relatively short to allow for a longer QNAME in the report query. The agent domain MUST NOT be a subdomain of the domain it is reporting on. That is, if the authoritative server hosts the foo.example domain, then its agent domain MUST NOT end in foo.example.

8.2. Managing Caching Optimizations

The reporting resolver may utilize various caching optimizations that inhibit subsequent error reporting to the same monitoring agent.

If the monitoring agent were to respond with NXDOMAIN (name error), [RFC8020] states that any name at or below that domain should be considered unreachable, and negative caching would prohibit subsequent queries for anything at or below that domain for a period of time, depending on the negative TTL [RFC2308].

Since the monitoring agent may not know the contents of all the zones for which it acts as a monitoring agent, the monitoring agent MUST NOT respond with NXDOMAIN for domains it is monitoring because that could inhibit subsequent queries. One method to avoid NXDOMAIN is to use a wildcard domain name [RFC4592] in the zone for the agent domain.

When the agent domain is signed, a resolver may use aggressive negative caching (described in [RFC8198]). This optimization makes use of NSEC and NSEC3 (without opt-out) records and allows the resolver to do the wildcard synthesis. When this happens, the resolver does not send subsequent queries because it will be able to synthesize a response from previously cached material.

A solution is to avoid DNSSEC for the agent domain. Signing the agent domain will incur an additional burden on the reporting resolver, as it has to validate the response. However, this response

has no utility to the reporting resolver other than dampening the query load for error reports.

9. Security Considerations

Use of DNS error reporting may expose local configuration mistakes in the reporting resolver, such as stale DNSSEC trust anchors, to the monitoring agent.

DNS error reporting SHOULD be done using DNS query name minimization [RFC9156] to improve privacy.

DNS error reporting is done without any authentication between the reporting resolver and the authoritative server of the agent domain.

Resolvers that send error reports SHOULD send them over TCP [RFC7766] or SHOULD use DNS Cookies [RFC7873]. This makes it hard to falsify the source address. The monitoring agent SHOULD respond to queries received over UDP that have no DNS Cookie set with a response that has the truncation bit (TC bit) set to challenge the resolver to requery over TCP.

Well-known addresses of reporting resolvers can provide a higher level of confidence in the error reports and potentially enable more automated processing of these reports.

Monitoring agents that receive error reports over UDP should consider that the source of the reports and the reports themselves may be false.

The method described in this document will cause additional queries by the reporting resolver to authoritative servers in order to resolve the report query.

This method can be abused by intentionally deploying broken zones with agent domains that are delegated to victims. This is particularly effective when DNS requests that trigger error messages are sent through open resolvers [RFC9499] or widely distributed network monitoring systems that perform distributed queries from around the globe.

An adversary may create massive error report flooding to camouflage an attack.

Though this document gives no guidance on the content of the RDATA in the TXT resource record, if the RDATA content is logged, the monitoring agent MUST assume the content can be malicious and take appropriate measures to avoid exploitation. One such method could be to log in hexadecimal. This would avoid remote code execution through logging string attacks, such as the vulnerability described in [CVE-2021-44228].

The rationale behind mandating DNSSEC validation for responses from a reporting agent, even if the agent domain is proposed to remain unsigned, is to mitigate the risk of a downgrade attack orchestrated by adversaries. In such an attack, a victim’s legitimately signed domain could be deceptively advertised as an agent domain by malicious actors. Consequently, if the validating resolver treats it as unsigned, it is exposed to potential cache poisoning attacks. By enforcing DNSSEC validation, this vulnerability is preemptively addressed.

10. References

10.1. 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/info/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/info/rfc8174>.

10.2. Informative References

[CVE-2021-44228] CVE, "CVE-2021-44228", 26 November 2021, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228>.

[MULTI-QTYPES] Bellis, R., "DNS Multiple QTYPEs", Work in Progress, Internet-Draft, draft-ietf-dnssd-multi-qtypes-00, 4 December 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-dnssd-multi-qtypes-00>.

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, DOI 10.17487/RFC2308, March 1998, <https://www.rfc-editor.org/info/rfc2308>.

[RFC4592] Lewis, E., "The Role of Wildcards in the Domain Name System", RFC 4592, DOI 10.17487/RFC4592, July 2006, <https://www.rfc-editor.org/info/rfc4592>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

[RFC7766] Dickinson, J., Dickinson, S., Bellis, R., Mankin, A., and D. Wessels, "DNS Transport over TCP - Implementation Requirements", RFC 7766, DOI 10.17487/RFC7766, March 2016, <https://www.rfc-editor.org/info/rfc7766>.

[RFC7873] Eastlake 3rd, D. and M. Andrews, "Domain Name System (DNS) Cookies", RFC 7873, DOI 10.17487/RFC7873, May 2016, <https://www.rfc-editor.org/info/rfc7873>.

[RFC8020] Bortzmeyer, S. and S. Huque, "NXDOMAIN: There Really Is Nothing Underneath", RFC 8020, DOI 10.17487/RFC8020, November 2016, <https://www.rfc-editor.org/info/rfc8020>.

[RFC8198] Fujiwara, K., Kato, A., and W. Kumari, "Aggressive Use of DNSSEC-Validated Cache", RFC 8198, DOI 10.17487/RFC8198, July 2017, <https://www.rfc-editor.org/info/rfc8198>.

[RFC8914] Kumari, W., Hunt, E., Arends, R., Hardaker, W., and D. Lawrence, "Extended DNS Errors", RFC 8914, DOI 10.17487/RFC8914, October 2020, <https://www.rfc-editor.org/info/rfc8914>.

[RFC9156] Bortzmeyer, S., Dolmans, R., and P. Hoffman, "DNS Query Name Minimisation to Improve Privacy", RFC 9156, DOI 10.17487/RFC9156, November 2021, <https://www.rfc-editor.org/info/rfc9156>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/info/rfc9499>.

Acknowledgements

This document is based on an idea by Roy Arends and David Conrad. The authors would like to thank Peter van Dijk, Stephane Bortzmeyer, Shane Kerr, Vladimir Cunat, Paul Hoffman, Philip Homburg, Mark Andrews, Libor Peltan, Matthijs Mekking, Willem Toorop, Tom Carpay, Dick Franks, Ben Schwartz, Yaron Sheffer, Viktor Dukhovni, Wes Hardaker, James Gannon, Tim Wicinski, Warren Kumari, Gorry Fairhurst, Benno Overeinder, Paul Wouters, and Petr Spacek for their contributions.

Authors' Addresses

Roy Arends
ICANN
Email: roy.arends@icann.org

Matt Larson
ICANN
Email: matt.larson@icann.org