DNS Error Reporting

Abstract

DNS Error Reporting is a lightweight error reporting mechanism that
provides the operator of an authoritative server with reports on DNS
resource records that fail to resolve or validate, that a Domain
Owner or DNS Hosting organization can use to improve domain hosting.
The reports are based on Extended DNS Errors [RFC8914].

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 recursive resolver
to automatically signal an error to an agent specified by the
authoritative server. DNS Error Reporting uses the DNS to report
errors.

Another lack of feedback occurs when validation was successful, or
when there is no error to report. This positive feedback may be
helpful to show that a deployment was successful. This document
introcudes an extended DNS error "NO ERROR".

Status of This Memo

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 recursive resolver will fail to validate these resource records.

Similarly, when there is a mismatch between the DS records at a parent zone and the key signing key at the child zone, a validating recursive 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.

There is no direct relationship between operators of validating recursive resolvers and authoritative servers. Outages are often noticed indirectly, by end users, and reported via 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 is buried in log files of the validating resolver, if these errors are logged at all.

This document describes a facility that can be used by validating recursive resolvers to report errors in an automated way. In addition, successful validation, or a lack of errors can also be reported in an automated way.

It allows an authoritative server to signal a reporting agent where the validating recursive resolver can report issues if it is configured to do so. The signal also indicates that the reporting agent is interested in successful validation, or lack of errors.

The burden of reporting a failure falls on the validating recursive 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", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Terminology

Reporting Resolver: In the context of this document, the term reporting resolver is used as a shorthand for a validating recursive resolver that supports DNS Error Reporting.

Reporting Query: The DNS query used to report an error is called a reporting query. A reporting query is for DNS resource record type NULL. The details of the error report are encoded in the QNAME of the reporting query.

Reporting Agent: A facility responsible for receiving error reports on behalf of authoritative servers. This facility is indicated by a domain name.

Reporting Agent Domain: a domain name which the reporting resolver includes in the QNAME of the reporting query.

Positive Feedback: A report that indicates that no error occurred.

4. Overview

An authoritative server indicates support for DNS Error Reporting by
including an EDNS0 option with OPTION-CODE [TBD] [RFC Editor: change
TBD to the proper code when assigned by IANA.], a flag to indicate a
request for positive feedback and the REPORTING AGENT DOMAIN in DNS
wireformat in the option's payload. The authoritative server MUST
NOT include this option in the response if the configured reporting
agent domain is empty or the null label (the root).

The positive feedback flag indicates that the reporting agent wants
to receive extended DNS error [TBD] that indicates that no error
occurred. This extended DNS error is defined in this document.

When a reporting resolver sends a reporting query to report an
error, it MUST NOT include the EDNS0 Error Reporting option in the
reporting query. This avoids additional compounding error reporting
when there is an issue with the reporting agent domain.

To report an error, the reporting resolver encodes the error report
in the QNAME of the reporting query. The reporting resolver builds
this QNAME by concatenating the _er label, the extended error code
[RFC8914], the QTYPE and the QNAME that resulted in failure, the
label "_er" again, and the reporting agent domain. See the example
in section 4.2.

The resulting concatenated domain name is sent as a standard DNS
query for DNS resource record type NULL by the reporting resolver.
This query MUST NOT have the EDNS0 option code [TBD] set to avoid
compounding error notifications.

The query will ultimately arrive at the authoritative server for the
reporting agent domain. A NODATA negative response is returned by
the authoritative server of the reporting agent domain, which in
turn can be cached by the reporting resolver.

This caching is essential. It ensures that the number of reports
sent by a reporting resolver for the same problem is dampened, i.e.
once per TTL, however, certain optimizations such as [RFC8020] and
[RFC8198] may reduce the number of error reporting queries as well.

4.1. Managing Caching Optimizations

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

If the authoritative server for the reporting agent domain were to
respond with NXDOMAIN (name error), [RFC8020] rules state 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 authoritative server for an agent domain may not know the contents of all the zones it acts as an agent for, it is essential that the authoritative server does not respond with NXDOMAIN, as that may inhibit subsequent queries. The use of a wildcard domain name [RFC4592] in the zone for the agent domain will ensure the RCODE is consistently NOERROR.

Considering the Resource Record type for this wildcard record, type NULL is prohibited in master zone files [RFC1035]. However, any type that is not special according to [RFC4592] section 4 will do, such as a TXT record with an email address for the reporting agent in the RDATA.

Wildcard expansion occurs, even if the QTYPE is not for the type owned by the wildcard domain name. The response is a "no error, but no data" response ([RFC4592], section 2.2.1.) that contains a NOERROR RCODE and empty answer section. Note that reporting resolvers are not expected to query for this TXT record, since reporting queries use type NULL. This record is solely present to ensure a NODATA response is returned in response to reporting queries.

When the zone for the reporting agent domain is signed, a resolver may utilize aggressive negative caching, discussed 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 may not send subsequent queries as it will be able to synthesize a response from previously cached material.

A solution is to avoid DNSSEC for the reporting 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.

4.2. Example

The domain broken.test is hosted on a set of authoritative servers. One of these serves a stale version. This authoritative server has a severity level of 1 and a reporting agent configured: a01.reporting-agent.example.

The reporting resolver is unable to validate the broken.test RRSet for type A, due to an RRSIG record with an expired signature.

The reporting resolver constructs the QNAME _er.
7.1.broken.test._er.a01.reporting-agent.example and resolves it.
This QNAME indicates extended DNS error 7 occurred while trying to
validate broken.test type 1 (A) record.

After this query is received at one of the authoritative servers for
the reporting agent domain (a01.reporting-agent.example), the
reporting agent (the operators of the authoritative server for
a01.reporting-agent.example) determines that the authoritative
server for the broken.test zone suffers from an expired signature
record (extended error 7) for type A for the domain name
broken.test. The reporting agent can contact the operators of
broken.test to fix the issue.

5. EDNS0 Option Specification

This method uses an EDNS0 [RFC6891] option to indicate support for
sending DNS error reports and responding with the Reporting Agent
Domain in DNS messages. The option is structured as follows:

```
                      1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |        OPTION-CODE = TBD       |        OPTION-LENGTH          |
 +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 |F|                REPORTING AGENT DOMAIN                       /
 +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

Field definition details:

   *OPTION-CODE, 2-octets/16-bits (defined in [RFC6891]), for
    indicating error reporting support is TBD. [RFC Editor: change
    TBD to the proper code when assigned by IANA.]

   *OPTION-LENGTH, 2-octets/16-bits ((defined in [RFC6891]) contains
    the length of the REPORTING AGENT DOMAIN field in octets.

   *F, A flag to request positive feedback (i.e. to include the "No
    Error" extended DNS error defined in this document when
    reporting).

   *REPORTING AGENT DOMAIN, a Domain name [RFC8499] in the DNS wire
    format prescribed by [RFC1035].

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 an error and what is not.

The DNS class is not specified in the error report.

6.1. Reporting Resolver Specification

Reporting Resolvers may have a configuration that allows the following:

The reporting resolver MUST NOT use DNS error reporting to report a failure in resolving the reporting query.

The reporting resolver MUST NOT use DNS error reporting if the authoritative server has an empty Reporting Agent Domain field in the EDNS Error Reporting option.

The reporting resolver should limit the amount of positive feedback send.

6.1.1. Constructing the Reporting Query

The QNAME for the reporting query is constructed by concatenating the following elements, appending each successive element in the list to the right-hand side of the QNAME:

*A label containing the string "_er".

*The Extended DNS error, presented as a decimal value, in a single DNS label.

*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.

*The QNAME that was used in the query that resulted in the extended DNS error. The QNAME may consist of multiple labels and is concatenated as is, i.e. in DNS wire format.

*A label containing the string "_er".

*The reporting agent domain. The reporting agent domain consists of multiple labels and is concatenated exactly as received in the EDNS option sent by the authoritative server.

If the resulting reporting query QNAME would exceed 255 octets, it MUST NOT be sent.

The "_er" labels allow the reporting agent to quickly differentiate between the agent domain and the faulty query name. When the specified agent domain is empty, or a NULL label (despite being not allowed in this specification), the reporting query will have "_er" as a top-level domain as a result and not the original query.

Lastly, the purpose of the first "_er" label is to indicate that a
complete reporting query has been received, instead of a shorter
reporting query due to query minimization.

6.2. Authoritative Server Specification

The Authoritative Server SHOULD NOT have multiple reporting agent
domains configured for a single zone. To support multiple reporting
agents, a single agent can act as a syndicate to subsequently inform
additional agents.

An authoritative server for a zone with DNS error reporting enabled
SHOULD NOT also be authoritative for that zone's reporting agent
domain's zone.

6.3. Reporting Agent Specification

It is RECOMMENDED that the reporting agent zone uses a wildcard DNS
record of type TXT with an arbitrary string in the RDATA and a TTL
of at least one hour.

6.4. Choosing a Reporting Agent Domain

It is RECOMMENDED that the reporting agent domain be kept relatively
short to allow for a longer QNAME in the reporting query.

7. IANA Considerations

IANA is requested to assign the following DNS EDNS0 option code
registry:

```
   Value    Name              Status     Reference
   -----    ---------------   --------   ---------------
   TBD      DNS ERROR REPORT  Standard   [this document]
```

[RFC Editor: change TBD to the proper code when assigned by IANA.]

IANA is requested to assign the following Underscored and Globally
Scoped DNS Node Name registry:

```
   RR Type  _NODE NAME  Reference
   -----    ----------  ---------
   TXT      _er         [this document]
```

IANA is requested to assign the following value the "Extended DNS
Error Codes" registry:

INFO-CODE: [TBD]

Purpose: No Error

Reference: This document

8. Security Considerations

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

    DNS Error reporting SHOULD be done using DNS Query Name Minimization
    [RFC7816] to improve privacy.

    DNS Error Reporting is done without any authentication between the
    reporting resolver and the authoritative server of the agent domain.
    Authentication significantly increases the burden on the reporting
    resolver without any benefit to the reporting agent, authoritative
    server or reporting resolver.

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

    This method can be abused by deploying broken zones with agent
    domains that are delegated to servers operated by the intended
    victim in combination with open resolvers [RFC8499].

9. Acknowledgements

    This document is based on an idea by Roy Arends and David Conrad.
    The authors would like to thank Peter van Dijk, Vladimir Cunat, Paul
    Hoffman, Libor Peltan, Matthijs Mekking, Willem Toorop, Tom Carpay,
    Dick Franks, Benno Overeinder and Petr Spacek for their
    contributions.

10. Informative References

    [RFC1035] Mockapetris, P., "Domain names - implementation and
               specification", STD 13, RFC 1035, DOI 10.17487/RFC1035,
               November 1987, <https://www.rfc-editor.org/info/rfc1035>.

    [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>.

[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>.

[RFC7816] Bortzmeyer, S., "DNS Query Name Minimisation to Improve
           Privacy", RFC 7816, DOI 10.17487/RFC7816, March 2016,
           <https://www.rfc-editor.org/info/rfc7816>.

[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>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS
           Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499,
           January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[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>.

Authors' Addresses

Roy Arends
ICANN

Email: roy.arends@icann.org

Matt Larson
ICANN

Email: matt.larson@icann.org