Domain Name System Operations
Internet-Draft
Intended status: Informational
Expires: August 22, 2019

J. Livingood
Comcast

February 18, 2019

In Case of DNSSEC Validation Failures, Do Not Change Resolvers
draft-livingood-dnsop-dont-switch-resolvers-04

Abstract

DNS Security Extensions (DNSSEC) validation by recursive DNS resolvers has been deployed at scale. However, domain signing tools and processes are not yet as mature and reliable as is the case for non-DNSSEC-related domain administration tools and processes. This sometimes results in DNSSEC validation failures, for which operators of validating resolvers are often blamed. When these failures do occur, end users should not change to a non-validating DNS resolver, as that would downgrade their security. They should instead wait until the authoritative domain operator updates their DNS records to resolve the error and that change propagates across the Internet's DNS resolvers, the timing of which may be dependent upon the Time To Live (TTL) settings in the old and/or erroneous DNS resource records.

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 August 22, 2019.

Table of Contents

1. Introduction

The Domain Name System (DNS), DNS Security Extensions (DNSSEC), and related operational practices are defined extensively [RFC1034] [RFC1035] [RFC4033] [RFC4034] [RFC4035] [RFC4398] [RFC4509] [RFC6781] [RFC5155].

DNS Security Extensions (DNSSEC) validation by recursive DNS resolvers has been deployed at scale. However, domain signing tools and processes are not yet as mature and reliable as is the case for non-DNSSEC-related domain administration tools and processes. This sometimes results in DNSSEC validation failures, for which operators of validating resolvers are often blamed.

When these DNSSEC validation failures do occur, end users SHOULD NOT change to a non-validating DNS resolver, as that would downgrade their security. They should instead wait until the authoritative domain operator updates their DNS records to resolve the error and then for that change to propagate across the Internet's DNS

resolvers, the timing of which may be dependent upon the Time To Live (TTL) settings in the old and/or erroneous DNS resource records.

This document is necessary because it has become commonplace for reporters, technical users, and others to recommend that people change to non-validating resolvers when a DNSSEC validation failure occurs. This is NOT a recommended practice, it actively downgrades user security, and it reduces the incentives for authoritative domain operators to improve their DNSSEC-related domain administration tools and processes.

As a result, this document provides an authoritative reference point to recommend that users SHOULD NOT change DNS resolvers when DNSSEC validation failures occur. Such errors may be due to genuine security problems, which DNSSEC validation was designed to protect against. In the same way that a Transport Layer Security (TLS) [RFC8446] certificate failure should not be bypassed or ignored, so too that DNSSEC validation failures should not be bypassed or ignored.

2. Reasons for DNSSEC Validation Failure

A domain name can fail DNSSEC validation for two general reasons: an actual security failure such as due to an attack or compromise of some sort, or as a result of misconfiguration (mistake) on the part of a domain administrator. There is no way for an average end user to discern which of these issues has caused a DNSSEC-signed domain to fail validation, and so end users should therefore assume that it is due to an actual security problem as the most conservative and security-protective approach.

3. Misunderstanding DNSSEC Validation Failures

End users may incorrectly interpret the failure to reach a domain due to DNSSEC-related misconfiguration as their ISP or DNS resolver operator purposely blocking access to the domain, or as a performance-related failure on the part of that ISP or DNS resolver operator. In reality, these failures may be due to a security issue of which the end user is not aware. If a user ignores such a failure, or is instructed to ignore it, and switches to a non-validating resolver, they may be subject to the risk of malware exposure, phishing attack, and so on. The root cause of a DNSSEC validation failure lies not with a recursive DNS operator but with the authoritative domain name owner or administrator [I-D.draft-livingood-dnsop-auth-dnssec-mistakes].

4. Comparison to Other DNS Misconfigurations

Authoritative DNS-related mistakes and errors typically affect the entire Internet, and all DNS recursive resolver operators equally. So for example, in an A record is incorrect, an end user would get the incorrect record in a DNS response no matter what resolver they used.

In contrast to this, DNSSEC-related mistakes, errors, or other validation security failures would only affect end users of those validating resolvers. That being said, different validating resolver operators may configure their servers slightly differently, have different server software, or have different server configurations, which can result in slightly different resolver validation behavior. It can also be the case that one resolver has cached a DNS resource record according to the TTL set by the authoritative domain administrator, while another resolver does not have that record cached (generally due to the timing of prior user queries for that name), which can also cause two resolvers to differ. Another reason for resolution variance may be that the authoritative DNS servers are responding differently to various DNS resolvers, perhaps to geographic differences, the nature of any delegations to Content Delivery Networks (CDNs), a regionally-focused Denial of Service (DoS) attack against an authoritative server, or a wide range of other potential reasons.

5. Switching to a Non-Validating Resolver is NOT Recommended

As noted in Section 3 some end users may not understand why a domain fails to validate on one network but not another (or with one DNS resolver but not another) Section 4. As a result, they may consider or someone may recommend to them switching to an alternative, non-validating resolver themselves. But if a domain fails DNSSEC validation and is inaccessible, this could very well be due to a security-related issue. Changing to a non-validating resolver is a critical security downgrade and is NOT advised.

DNSSEC validation failures may be due to genuine security problems, which DNSSEC validation was designed to protect against. In the same way that a Transport Layer Security (TLS) [RFC8446] certificate failure should not be bypassed or ignored, so too that DNSSEC validation failures should not be bypassed or ignored.

As a recommended best practice: In order to be as safe and secure as possible, end users SHOULD NOT change to DNS resolvers that do not perform DNSSEC validation as a workaround when DNSSEC validation failures occur.

Even if a website in a domain seems to look "normal" and valid, according to the DNSSEC protocol, that domain is not secure. Domains that fail DNSSEC validation may fail due to an actual security incident or compromise, and may be in control of hackers or there could be other significant security issues with the domain. Thus, switching to a non-validating resolver to restore access to a domain that fails DNSSEC validation is NOT recommended and is potentially harmful to end user security.

6. Other Considerations

6.1. Recommendations for Validating Resolver Operators

Since it is not recommended that end users change to non-validating resolvers, operators of validating resolvers may wish to consider what tools they might make available to their end users to assist in these cases. For example, there may be a DNS looking glass that enables someone to use a web page or other tool to remotely (including from a different network) check DNS resolution on the operator's servers, as well as possibly another operator's servers. Such a web page or tool may also provide a link to independent third party sites or tools that can confirm whether or not a DNSSEC-related error is present, of which several exist today (e.g. DNSViz [1], Verisign DNSSEC Debugger [2]). Finally, the operator may also wish to consider a web page form or other tool to enable end users to report possible DNS resolution issues.

Resolver operators may also find it helpful to selectively use a Negative Trust Anchor [RFC7646] to temporarily mitigate validation failures that are absolutely confirmed to be due to authoritative domain name administration error by that administrator. In addition, in select cases such as a very high traffic domain name, once an administrative DNS error or problem has been fixed a resolver may consider clearing the cache of their recursive resolvers in order to pickup the authoritative change immediately (rather than waiting until the TTL on a cached record expires).

6.2. Security Considerations

The use of a non-validating DNS recursive resolver is comparatively less secure than using a validating resolver, since one implements DNS Security Extensions (DNSSEC) and one does not.

In the case of a DNSSEC validation failure, if an end user changes to a non-validating resolver they can subject themselves to increased security risks and threats against which DNSSEC may have provided protection.

As a result, in order to protect their security, users SHOULD NOT switch to a non-validating resolver when a DNSSEC validation failure occurs.

6.3. Privacy Considerations

In the case of a DNSSEC validation failure, if an end user changes to a non-validating resolver they can subject themselves to increased security risks and threats against which DNSSEC may have provided protection. This can include threats to their privacy, such as by unwittingly visiting a phishing site and sharing sensitive data or other private information with a malicious party or some party other than that which was originally intended.

As a result, in order to protect their privacy, users SHOULD NOT switch to a non-validating resolver when a DNSSEC validation failure occurs.

6.4. IANA Considerations

There are no IANA considerations in this document.

7. Acknowledgements

- William Brown

- Peter Koch

8. References

8.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[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>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC4398] Josefsson, S., "Storing Certificates in the Domain Name System (DNS)", RFC 4398, DOI 10.17487/RFC4398, March 2006, <https://www.rfc-editor.org/info/rfc4398>.

[RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, DOI 10.17487/RFC4509, May 2006, <https://www.rfc-editor.org/info/rfc4509>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/info/rfc5155>.

[RFC5914] Housley, R., Ashmore, S., and C. Wallace, "Trust Anchor Format", RFC 5914, DOI 10.17487/RFC5914, June 2010, <https://www.rfc-editor.org/info/rfc5914>.

[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, DOI 10.17487/RFC6781, December 2012, <https://www.rfc-editor.org/info/rfc6781>.

[RFC7646] Ebersman, P., Kumari, W., Griffiths, C., Livingood, J., and R. Weber, "Definition and Use of DNSSEC Negative Trust Anchors", RFC 7646, DOI 10.17487/RFC7646, September 2015, <https://www.rfc-editor.org/info/rfc7646>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

8.2. Informative References

[I-D.livingood-dnsop-auth-dnssec-mistakes] Livingood, J., "Responsibility for Authoritative DNSSEC Mistakes", draft-livingood-dnsop-auth-dnssec-mistakes-03 (work in progress), November 2015.

8.3. URIs

[1] http://dnsviz.net/

[2] http://dnssec-debugger.verisignlabs.com/

Appendix A. Document Change Log

[RFC Editor: This section is to be removed before publication]

Individual-00: First version published as an individual draft.

Individual-01: Fixed nits identified by William Brown

Individual-02: Updated prior to IETF-91

WG-00: Renamed at request of DNSOP co-chairs

WG-01: Updated doc to keep it from expiring

WG-02: Addressed some feedback from Peter Koch on RFC 2119 text, changed from BCP to Informational since this is more a recommended practice, added a section with recommendations for operators.

WG-03 to 04: Refreshed document

Appendix B. Open Issues

[RFC Editor: This section is to be removed before publication]

Fix I-D xref

Author's Address

Jason Livingood
Comcast

Email: jason_livingood@comcast.com