Zeros Are Heroes: NSEC3 Parameter Settings in the Wild

Cordian Alexander Daniluk, Yevheniya Nosyk, Andrzej Duda, Maciej Korczyński

Zeros Are Heroes: NSEC3 Parameter Settings in the Wild

Cordian Alexander Daniluk*
Hasso Plattner Institute, University of Potsdam
Potsdam, Germany
cordian.daniluk@grenoble-inp.org

Yevheniya Nosyk
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
Grenoble, France
yevheniya.nosyk@univ-grenoble-alpes.fr

Andrzej Duda
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
Grenoble, France
andrzej.duda@univ-grenoble-alpes.fr

Maciej Korczyński
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
Grenoble, France
maciej.korczynski@univ-grenoble-alpes.fr

Abstract

Domain Name System Security Extensions (DNSSEC) enhanced the security of conventional DNS by providing data integrity and origin authentication, but enabled zone walking as a side effect. To address this issue, the Next Secure (NSEC3) resource record provides an authenticated denial of existence mechanism based on hashes of domain names. However, an improper selection of the NSEC3 parameters may significantly degrade the performance of resolvers and authoritative name servers alike. RFC 9276 (Guidance for NSEC3 Parameter Settings) imposes additional constraints on hash computation parameters, crucial in light of emerging security threats such as CPU resource exhaustion attacks. Despite this guideline, our analysis of over 302 M registered domain names reveals that 87.8 % of 15.5 M NSEC3-enabled domains fail to adhere to RFC 9276 with a dozen using 500 additional hash iterations. Furthermore, 78.3 % of 114 K open and closed validating resolvers impose the RFC's additional constraints on hash iterations with 18.4 % returning SERVFAIL, possibly rendering non-compliant domains unreachable.

ACM Reference Format:
Cordian Alexander Daniluk, Yevheniya Nosyk, Andrzej Duda, and Maciej Korczyński. 2024. Zeros Are Heroes: NSEC3 Parameter Settings in the Wild. In *Proceedings of the 2024 ACM Internet Measurement Conference (IMC '24), November 4–6, 2024, Madrid, Spain.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3646547.3689017

1 Introduction

The Domain Name System was introduced in 1987 [43, 44] to associate human-readable domains with network addresses in a scalable manner. However, it was not designed with security in mind, which makes it fundamentally vulnerable to tampering attacks [5, 28, 37, 53]. DNS Security Extensions (DNSSEC) [59–61] added origin authentication and data integrity to standard DNS based on public-key cryptography.

As acknowledged but not addressed in RFC 4033 [59], the denial-of-existence mechanism offered by the Next Secure (NSEC) DNS record facilitates zone walking, a concern for domain operators aiming to keep their zone confidential. Moreover, DNSSEC requires that every delegation point to an unsigned zone owns an NSEC record. This increases the required effort to resign zone files, especially in large delegation-oriented zones. To remedy these two problems, RFC 5155 (DNS Security Hashed Authenticated Denial of Existence) [4] replaced NSEC with a new NSEC3 record that does not contain plain domain names but their hashes.

A per-zone set of parameters determines the exact procedure for NSEC3 hash computation: the hash algorithm, the number of additional hash iterations, and the length of the salt appended to the intermediate result of every iteration. While these measures exist to protect against offline dictionary attacks, RFC 5155 acknowledged that a large number of iterations could negatively affect the performance of authoritative name servers and validating resolvers. Therefore, it imposed upper limits on the number of hash iterations. Beyond these limits, a validating resolver may consider the received data insecure.

In 2021, the DNS operator community started questioning the usefulness of any iteration value beyond one and the use of the salt altogether [68]. It was argued that a single iteration is enough to discourage most zone walking, since many subdomains are easily guessable in any case, e.g., www or api. Furthermore, as the hashed data includes the zone's name, it acts as a per-zone salt and reduces the importance of the corresponding salt field. These concerns culminated in RFC 9276 (Guidance for NSEC3 Parameter Settings) [26], which, among other things, forbids the use of *any* additional iterations and discourages the use of a salt.

In early 2024, CVE-2023-50868 highlighted how DNSSEC-signed domains with high iteration values can substantially slow down the performance of validating resolvers [3]. Gruza et al. [24] experimentally verified that it can increase the resolver CPU instruction count by up to 72 times. These findings advocate the urgent implementation of RFC 9276. However, no existing work systematically analyzed the adoption of this best current practice across a large set of domain names and validating resolvers. Our paper aims at filling this research gap and presents the following contributions:

- We analyze 1,449 top-level domains (TLDs) and uncover that 447 used as many as 100 additional iterations as of March 2024, all managed by one TLD registry services provider.

*This work was done while Cordian Alexander Daniluk was an intern at Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG.

IMC '24, November 4–6, 2024, Madrid, Spain

ACM ISBN 979-8-4007-0592-2/24/11
https://doi.org/10.1145/3646547.3689017

Those were subsequently reduced to 0, as required by the best current practice.
- We perform a large-scale measurement of more than 302 M registered domains and show that as many as 87.8 % of 15.5 M NSEC3-enabled domains do not comply with RFC 9276.
- We set up 49 subdomains under `rfc9276-in-the-wild.com` to determine how validating resolvers treat domains with various iteration counts from 1 to 500. We make this infrastructure open for the community to use.
- We analyze 1.9 M open and 2.5 K closed IPv4/IPv6 resolvers, the latter using RIPE Atlas. We show that 78.3 % of 114 K DNSSEC validators limit the number of additional iterations they process. Furthermore, 18.4 % of validating resolvers take a strict approach and return SERVFAILs for domains with non-zero iteration counts. As 418 resolvers do not accept any additional iteration count higher than 0, they potentially render 13.6 M domains unavailable to end users.

The rest of the paper is organised as follows. Section 2 provides the necessary background on DNSSEC, denial of existence, and best practices for NSEC3 parameter settings. Section 3 discusses the related work in the field. Section 4 describes the measurement methodology and Section 5 presents the results. We conclude the paper in Section 6.

2 Background

This section offers essential information on DNSSEC, authenticated denial of existence, and best practices for NSEC3 parameter settings as per RFC 9276.

2.1 Primer on DNSSEC

Domain Name System Security Extensions (DNSSEC) [59–61] integrate authentication and integrity features into conventional DNS through public-key cryptography.

Domain owners typically manage two key pairs for operational purposes: the zone signing key pair for signing all the zone data and the key signing key pair to sign the public keys themselves. As a result, the newly added DNSKEY resource record stores public keys while the RRSIG record stores the signatures over RRsets [61].

The role of a DNSSEC-validating resolver is to assess the integrity and authenticity of the data it receives. This trust is of utmost importance. If misplaced, an attacker could potentially carry out various malicious activities, including intercepting queries and injecting false responses into the DNS resolution process [47]. To ensure this trust, DNSSEC establishes a mechanism in which parent zones attest the trustworthiness of keys within child zones: the parent zone publishes the hash of the key signing key of the child zone in a DS record signed by the zone signing key of the parent zone itself. Repeating this scheme yields an authentication chain—an alternating sequence of DNSKEY and DS records. The root zone is at the top of the DNSSEC hierarchy, serving as the trust anchor for cryptographic validation of DNS responses globally. A response is considered valid by the DNSSEC-validating resolver as long as an authentication chain exists from a given RRSIG to the root.

Table 1: RFC 9276 guidelines for authoritative name servers (1–5) and validating resolvers (6–12).

Item	Keyword	Guidance
1.	**SHOULD**	prefer NSEC over NSEC3, if the NSEC3 operational or security features are not needed
2.	**MUST**	set the number of additional iterations to 0
3.	**SHOULD NOT**	use a salt
4.	**NOT RECOMMENDED**	to set the opt-out flag for small zones
5.	**MAY**	set the opt-out flag for very large and sparsely signed zone with the majority of records insecure delegations
6.	**MAY**	return an insecure response if a queried name server returns NSEC3 resource records (RR) not complying with Item 2
7.	**MUST**	verify the RRSIG RRs for NSEC3 RRs in the answer of the authoritative server to ensure integrity of the number of additional iterations, if Item 6 is implemented
8.	**MAY**	set RCODE to SERVFAIL in the response to the client, if a queried name server returns NSEC3 RRs not complying with Item 2
9.	**MAY**	ignore the response of the queried name server, if it returns NSEC3 RRs not complying with Item 2, likely resulting in setting RCODE to SERVFAIL in the response to the client
10.	**SHOULD**	return EDE information with INFO-CODE set to 27, if Item 6 or Item 8 are implemented
11.	**MUST NOT**	return EDE information as in Item 10, if Item 9 is implemented
12.	**SHOULD**	set the number of iterations starting from which Item 6 and Item 8 are implemented to the same value if both are implemented

2.2 Denial of Existence

The validation process cannot prove the non-existence of a DNS record or a subdomain, since without any data, there is nothing for an RRSIG record to cover and authenticate. Nevertheless, attackers must be prevented from injecting negative responses. To that end, the Next Secure (NSEC) record was added. It contains the next existing domain name according to the canonical order defined in RFC 4034 [61]. Additionally, it includes all the resource record types at the owner domain name, thereby demonstrating that nothing exists in between. Each domain name that owns authoritative data or is a delegation point has the corresponding NSEC record.

One can recursively look up NSEC resource records of a domain name to enumerate all subdomains in a zone. NSEC3 prevents such a simple reconnaissance technique by storing the hashes of domains in a new NSEC3 record, unlike the plain text domain names in NSEC. The canonical order is replaced by the order of the hash numeric values.

Each NSEC3 record defines the parameters used for hash computation: the hash algorithm, the number of additional iterations of the hash function, and the salt value appended to the domain name. In addition, each NSEC3 record stores an opt-out flag, indicating whether NSEC3 may cover a delegation point that owns no NSEC3 record itself. An NSEC3PARAM resource record defines the very same NSEC3 computation parameters. For all NSEC3 records in a given response, all their parameters have to be identical [4].

2.3 Guidance for NSEC3 Parameter Settings

Table 1 summarizes the guidelines for authoritative name servers (Items 1–5) and validators (Items 6–12) as described in RFC 9276. The rationale behind these best current practices is that if an attacker has enough resources for an offline dictionary attack, then

they will be able to guess most of the domains in the zone, independently of the number of additional hash iterations (Item 2). A similar point is made for the salt (Item 3): The salt effectiveness relies on its frequent rotation but due to the complexity of changing the salt, it cannot be rotated often enough, which makes it useless. Moreover, updating the salt is costly as it requires recomputing all hashes and replacing every NSEC3 record. More generally, subdomains are often easily predictable (e.g., www, ftp, api), so hiding them may not justify the effort put into zone signing and validation (Item 1).

3 Related Work

The deployment of DNSSEC has been studied across various dimensions, including domain names [66, 70], DNS operators [39], registrars [10], and resolvers [19, 25, 41, 72, 76]. Chung et al. [9] provided the most extensive analysis of the DNSSEC ecosystem to date but did not specifically focus on the denial of existence mechanisms.

Since the release of RFC 5155 in 2008, numerous issues with NSEC3 have come to light. Researchers have shown its ineffectiveness against zone walking [71, 73]. Papadopoulos et al. [51] proposed NSEC5, an alternative documented in an RFC draft [69] (currently expired) based on Verifiable Random Functions [21].

While numerous DoS techniques against DNS were discovered and documented [1, 2, 6, 27], one specifically targets the NSEC3 mechanism. Known as CVE-2023-50868, it makes a validating resolver verify the NSEC3 proofs of non-existence from domains with many hash iterations, hence increasing the load on the resolver. Gruza et al. analyzed the impact of the CVE with different settings of the salt length and the number of additional iterations [24]. Our work complements their study by quantifying how many resolvers are susceptible to such an exploit in reality. Moreover, we extend the domain analysis to 302 M registered domains and 1,449 TLDs. To the best of our knowledge, our study represents the first effort to systematically analyze NSEC3 parameter configurations across such a vast range of domain names and resolvers.

4 Methodology

This section outlines our methodology for assessing RFC 9276 compliance for both domain names and recursive resolvers.

4.1 Domain Names

We curate a large list of registered domain names from different sources, including generic TLD (gTLD) zone files from ICANN Centralized Zone Data Service (CZDS) [32], country-code TLD (ccTLD) zone files downloaded via AXFR zone transfers for ch, .nu, .se, and .li, Google Certificate Transparency logs [7], as well as a passive DNS feed from SIE Europe [62]. All the entries are aggregated and deduplicated, resulting in a list of 302 M unique registered domain names. Additionally, we analyze all 1,449 delegated top-level domains such as .com, .ch, or .bank [31].

In March 2024, we used zdns [36] to query each domain for its DNSKEY records using the Cloudflare resolver [11], which has previously served well for large-scale domain measurements [46]. If any DNSKEY records are returned, we consider the domain name DNSSEC-enabled. This method narrows down domains for further analysis. While this approach may discard some domains that have NSEC3 chains but no DNSKEYs, we argue that the fraction of such domains is small since the generation of NSEC3 records requires a signing key. We analyze all the domains with DNSKEY records, regardless of whether they are correctly signed or not.

Right afterwards, we queried all the DNSSEC-enabled domains for their NSEC3PARAM and NS records. They allow us to extract the NSEC3 parameters used to sign the domain and identify their authoritative name servers. As we cannot directly retrieve NSEC3 records, we query a random subdomain of each tested domain to trigger a negative response or the one generated from a wildcard expansion. We only keep the domains that have exactly one NSEC3PARAM record to create a one-to-one mapping between a domain and its NSEC3 parameters. We further check the compliance with RFC 5155, i.e., ensure that domains i) have consistent parameters among all the NSEC3 records, and ii) have consistent parameters among the NSEC3 and NSEC3PARAM records. We term these domains NSEC3-enabled and analyze their compliance with RFC 9276.

4.2 Validating Resolvers

We measure the adoption of RFC 9276 across open and closed recursive DNS resolvers in April 2024. To obtain the list of IPv4 open resolvers, we i) set up a custom domain name, ii) gather the list of all routable IPs [48], iii) send DNS A requests for unique subdomains under our scan domain, and iv) keep 1.4 M IP addresses responding with a NOERROR response code [38]. For IPv6, we rely on the IPv6 Hitlist service [20] to gather 509 K hosts with port 53 open (note that they may also include authoritative name servers). As closed resolvers are not reachable from outside the tested networks, we rely on RIPE Atlas [58]—a measurement network provided by RIPE NCC with vantage points placed all over the world. We identify probes with local resolvers that are closed.

We analyze the resolver compliance with RFC 9276 in two steps: i) we determine validating resolvers, and ii) we check their behavior when resolving domain names with varying numbers of additional iterations. For that purpose, we set up 49 NSEC3-enabled subdomains with no salt under rfc9276-in-the-wild.com, including a correctly signed subdomain (valid), a subdomain with expired signatures (expired), and subdomains with N additional iterations (it-N).

The distribution of values for N is modeled empirically: our measurements in Section 5.1 show that more than 99.9 % of NSEC3-enabled domains have at most 25 additional iterations. Thus, all values between 1 and 25 have corresponding subdomains. The other subdomains are chosen in steps of 25 until 500 included, the highest observed value. The values of 50, 100, and 150 are common limits for returning an insecure response (Item 6) or a SERVFAIL (Item 8) implemented by major DNS software vendors. More specifically, BIND9, Knot Resolver, PowerDNS Recursor, and Unbound started returning insecure responses for domain names with more than 150 iterations in 2021 [13, 33, 45, 54]. All except Unbound have further lowered this limit to 50 by the end of 2023 [15, 35, 55]. We also experimentally determine that Quad9 and Google Public DNS return insecure responses above 150 and 100 iterations, respectively. Cloudflare Resolver and Cisco OpenDNS return a SERVFAIL for domains with more than 150 iterations. Hence, we also set up three

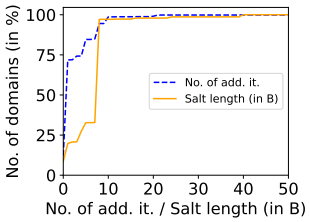


Figure 1: CDF of the salt length and the no. of additional iterations for all NSEC3-enabled domains.

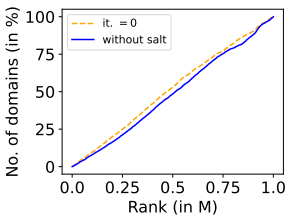


Figure 2: CDF of popularity ranks of NSEC3-enabled domains in the Tranco 1 M domain list.

subdomains for the successors 51, 101, and 151 to help us confirm the expected change in response codes.

Since the required action resulting from too many iterations is not strict in Item 9 (it "likely" results in a SERVFAIL), we exclude this point from our analysis. Whether or not such behavior still results in INFO-CODE 27 (Item 11) is therefore not checked either.

We set up a subdomain with 2,501 additional iterations (exceeding all limits set by RFC 5155 [4]) and an expired RRSIG signature covering the NSEC3 records (it-2501-expired). It allows detecting whether any validating resolver that returns an insecure response above a certain limit (Item 6) does not validate NSEC3 records with too many additional iterations. If we receive an NXDOMAIN instead of a SERVFAIL for this subdomain, a resolver does not verify the integrity of the NSEC3 record, violating Item 7.

All the subdomains additionally have wildcard records, so that each query we send contains a uniquely identifiable subdomain for each tested resolver. The valid subdomain, with zero additional iterations, complies with RFC 9276. Thus, we expect a validating resolver to return NOERROR with the AD bit set for valid and SERVFAIL for expired subdomains. All subdomains are reachable over both IPv4 and IPv6 addresses.

We enable server-side logging to track source IP addresses interacting with our name server. If the query destination is a forwarder, this helps identify the forwarding target by mapping the source IP to its originating AS and organization.

5 Evaluation

In this section, we evaluate the compliance of domain names and recursive resolvers with RFC 9276.

5.1 Domain Names

Overall, we analyze more than 302 M registered domain names and 1,449 TLDs, 26.6 M and 1,354 of those being DNSSEC-enabled. We concentrate our further analysis on 15.5 M domains and 1,302 TLDs that are NSEC3-enabled and check whether they follow Items 1–5 from Table 1.

Preference of NSEC over NSEC3: RFC 9276 recommends reviewing the necessity of supporting hashed authenticated denial of existence when it is not strictly essential for operational or security purposes (Item 1). While it is not evident from an external perspective whether the use of NSEC3 is justified, we argue that registered domains have little interest in preventing zone enumeration or

Table 2: The 10 most frequently encountered name server operators and the number of NSEC3-enabled domains they serve exclusively. All NSEC3 settings per organization represent at least 99.9 % of all exclusively served domains.

Auth. Name Server Operator	# of NSEC3-enabled domains (and in %)	# of additional iterations/ Salt length (in B)
Squarespace [22]	6,130,794 (39.4)	1/8
one.com [49]	1,472,149 (9.5)	5/5, 5/4, 1/2, 1/4
OVHcloud [50]	1,304,505 (8.4)	8/8
Wix.com [74]	783,790 (5.0)	1/8
TransIP [65]	647,792 (4.2)	0/8, 100/8
Loopia [42]	561,717 (3.6)	1/1
domainname.shop [17]	420,129 (2.7)	0/0
TimeWeb [64]	319,773 (2.1)	3/0
Hostnet [29]	225,431 (1.5)	1/4, 0/0
Hostpoint [30]	205,330 (1.3)	1/40

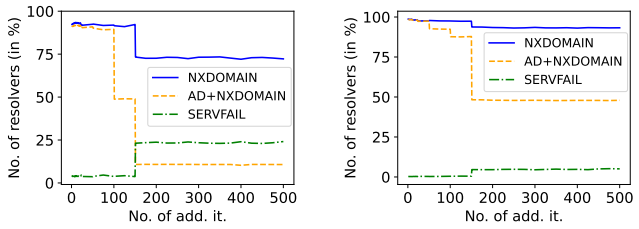
using the opt-out flag, except in specific cases. Given that 58.9 % of DNSSEC-enabled domains are NSEC3-enabled, this guideline is not widely followed. On the other hand, 1,302 out of 1,354 (96.2 %) DNSSEC-enabled TLDs use the NSEC3 mechanism. Out of them, at least 1,105 (84.9 %) publicly share their zone content via services such as CZDS, possibly still benefiting from the opt-out flag but rendering hashing of domains useless.

Number of additional iterations: Whenever domain owners choose to proceed with NSEC3, they are advised to set the number of additional iterations to zero (Item 2). Figure 1 shows the cumulative distribution of additional iterations for all the NSEC3-enabled registered domains. Alarmingly, only 12.2 % of domains have zero additional iterations, thus meeting the RFC 9276 requirement. While this value does not exceed 25 for 99.9 % of NSEC3-enabled domains, there are 43 domains on the long tail with more than 150 additional iterations, reaching up to 500 in 12 cases—the highest value observed.

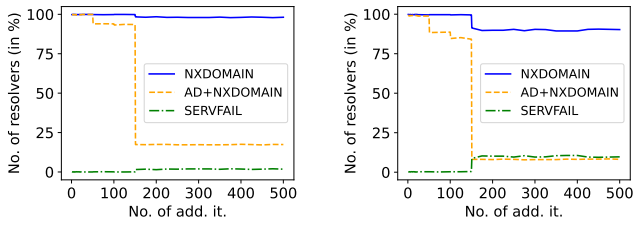
TLDs exhibit a significantly higher compliance ratio, with 688 using zero additional iterations. Interestingly, other 447 top-level domains have 100—the maximum value observed for TLDs. To assess the number of domains under those TLDs, we download corresponding zone files from CZDS [32] and, when unavailable, count domain names in our list of 302 M registered domains, which is necessarily incomplete and therefore only provides a lower bound. Overall, the aforementioned 447 TLDs account for at least 12.6 M domains in total. They are all managed by the Identity Digital registry services provider, having updated from 1 to 100 additional iterations in September 2020 [75]. Since the initial measurements were performed in March 2024, the additional iterations for all 447 TLDs have been reduced from 100 to 0, as required by RFC 9276.

Use of a salt: Similarly, domains should not use a salt (Item 3). Only 8.6 % of NSEC3-enabled domains do not have any salt. Whenever they do, it does not exceed 10 bytes in 97.2 % of cases as shown in Figure 1. On the long tail, 170 domains have salt lengths greater than 45 bytes, 9 of them with 160 bytes, and served by a single name server operator. Focusing on TLDs, while 672 do not use the salt, 558 have the 8-byte salt and 7 use 10 bytes, the maximum length observed.

Use of the opt-out flag: Another important aspect of the RFC 9276 is the use of the opt-out flag. We recall that the opt-out flag serves to omit NSEC3 records for insecure delegation points by



(a) Open, IPv4 (b) Open, IPv6



(c) Closed, IPv4 (d) Closed, IPv6

Figure 3: RCODEs of validating resolvers. Every subfigure shows the share of responses returning NXDOMAIN, SERVFAIL, and NXDOMAIN with the AD bit set.

having an NSEC3 record with the opt-out flag set covering that delegation point name. It is *not recommended* for small zones (Item 4), but *may* be set in large zones with many unsigned delegations (Item 5). As only 6.4 % (994 K) of registered NSEC3-enabled domains have the opt-out flag set in any of the returned NSEC3 records, we conclude that Item 4 is largely followed. On the contrary, TLD zones are very large and can have many insecure delegations. Thus, they have an incentive to set the opt-out flag—it is the case for 85.4 % of NSEC3-enabled TLDs. Hence, Item 5 is widely implemented for TLDs.

DNS operators supporting NSEC3: To analyze the distribution of authoritative name server operators serving (non-)compliant domains, we process the NS records of all the NSEC3-enabled domains and aggregate them by registered domains, even when under different public suffixes. Table 2 shows the 10 authoritative name server operators that exclusively serve 77.7 % of NSEC3-enabled domains, each associated with NSEC3 parameters occurring the most often. Google Domains (now acquired by Squarespace), the operator with the largest share, explicitly documents its choice of 1 and 8 for the number of additional iterations and the salt length [23]. TransIP, domainname.shop, and Hostnet map to zero additional iterations as required by Item 2 and only domainname.shop and Hostnet also have no salt as per Item 3. Out of all the NSEC3-enabled domains exclusively served by TransIP, 0.3 % use 100 iterations, which may be an artefact of the TransIP transition from 100 to 0 additional iterations [67] around 2021. In contrast to these measured values, the authoritative name server implementations BIND9, PowerDNS Authoritative Server, and Knot DNS [14, 34, 56] updated their default settings to zero additional iterations and no salt in the end of 2021, with only Knot DNS keeping a default salt length of 8 bytes.

Popular domains supporting NSEC3: Lastly, we analyze if popular domains respect the requirements in Item 2 (no additional iterations) and Item 3 (no salt). We intersect the Tranco domain popularity list [40], acquired on March 5, 2024[1], with NSEC3-enabled domains to assess compliance with both requirements (see Figure 2). The Tranco list contains 66.6 K DNSSEC-enabled domain names, out of which 27.2 K (40.8 %) are NSEC3-enabled. In turn, 6.2 K of them (22.8 %) have zero additional iterations and 6.4 K (23.6 %) do not have the salt. Both curves in Figure 2 increase uniformly, indicating that compliance (and therefore non-compliance) with Items 2 and 3 is uniformly distributed among the ranks. Only 3.5 K domains out of the 27.2 K (12.7 %) NSEC3-enabled popular domains comply with both.

Whether or not domains with many iterations remain reachable depends on the adoption of RFC 9276 by resolvers, which we examine below.

5.2 Validating Resolvers

Out of 1.9 M open and 2.5 K closed resolvers tested, we identify 105.2 K IPv4/6.8 K IPv6 open and 1,236 IPv4/689 IPv6 closed DNSSEC validators. Figure 3 shows the distributions of response codesm received for each of the `it-N` subdomains from open and closed validators. Three major response types are shown: i) NXDOMAIN, ii) NXDOMAIN with the `Authenticated Data` (AD) bit set (a subset of the first category), and iii) SERVFAIL.

Insecure responses for too many iterations: Overall, 59.9 % of the validating resolvers implement Item 6 from Table 1, meaning that they treat domains with high iteration values as insecure. Specifically, there exists a delimiting value N such that subdomains with up to N additional iterations result in NXDOMAIN responses with the AD bit set, while iteration counts above N result in NXDOMAIN only. Major resolvers were updated in 2021 to return insecure responses above 150 additional iterations, so a significant decrease in the number of NXDOMAIN responses with the AD bit set at 150 is consistent with these popular software implementations.

The other two common delimiting iteration values are 100 and 50, although less frequent that 150. The value of 50 coincides with the behavior of resolver implementations patched to protect from CVE-2023-50868. Across all the resolver types measured, there are 12.5 times fewer validators with this lowered iteration limit compared to the threshold of 150, meaning that these patches have not been widely applied yet. The value of 100 in turn is consistent with the behavior of Google Public DNS: 38.3 K open IPv4 resolvers (36.4 %) returned NXDOMAIN with the AD bit set for 100 iterations and cleared for 101.

SERVFAIL for too many iterations: Fewer validating resolvers (18.4 %) return SERVFAILs starting from some threshold N, meaning that they implement Item 8 from Table 1. For all types of resolvers tested, the first SERVFAIL mostly occurs at the additional iteration value of 151. As seen on our authoritative nameservers, some of those resolvers forward queries to Cloudflare and Cisco OpenDNS. As further shown in Figure 3, the number of SERVFAILs increases after 150 iterations and remains at this high level for every category of resolvers tested. Consequently, the number of NXDOMAINs decreases in proportion to the increase of SERVFAILs.

[1]Available at https://tranco-list.eu/list/588XN

The other two common starting points for SERVFAILs are 1 (418 resolvers) and 101 (92 resolvers), the great majority of those being open IPv4. While the limit of 100 only renders unreachable a tiny subset of domains (see Figure 1) the limit of 0 prevents access to 87.8 % of NSEC3-enabled domains if requesting non-existing records or subdomains. Most resolvers returning the SERVFAIL starting from it-1 only set the Recursion Available (RA) bit in responses if also set in queries. This indicates that they simply copy the query content to the response. Virtually all resolvers returning SERVFAIL starting from it-101 accompany the responses with the extended DNS error INFO-CODE 27 (Unsupported NSEC3 Iterations Value) and the EXTRA-TEXT, consistent with the behavior of the Technitium DNS Server [63].

EDE for too many iterations: More generally, less than 18 % of open resolvers returning insecure or SERVFAIL responses accompany them with an extended DNS error INFO-CODE 27, indicating a low support of Item 10. We have not analyzed closed resolvers, since RIPE Atlas does not supply the EDE data. Focusing on public resolvers, while Cloudflare does add the INFO-CODE 27, Google Public DNS and Cisco OpenDNS do not, yet returning INFO-CODE 5 (DNSSEC Indeterminate) and 12 (NSEC missing) instead. Quad9 returns insecure responses at the limit of 150 and does not return any extended DNS error code. The lack of INFO-CODE 27 is especially a problem for the resolvers returning SERVFAILs, since a client cannot distinguish a failure due to exceeding the iteration limit from the one returned for other reasons.

Verify insecure responses: RFC 9276 underscores the importance of validating the integrity of NSEC3 records before considering their additional hash iterations (Item 7). Therefore, we request every resolver returning insecure responses from a certain threshold N to resolve a subdomain with 2,501 additional iterations, but expired signatures over the NSEC3 RRset (it-2501-expired). We expect a correctly configured validator to return a SERVFAIL RCODE instead of NXDOMAIN. We encounter 0.2 % of validators exhibiting this non-compliant behavior.

Insecure responses and SERVFAIL at different limits: Provoking an insecure response via a downgrade attack by modifying the response to include existing NSEC3 records with high iteration values disables DNSSEC authentication [4]. Item 12 in Table 1 warns from not setting the same threshold for returning insecure responses and SERVFAILs to avoid an interval of iteration values, for which such a downgrade attack would be possible. We detected 4.3 % of validators first returning NXDOMAIN responses without the AD bit at some delimiting point N and then returning SERVFAILs at a higher point M, thus leaving a gap between the two. However, querying these resolvers again often results in different response patterns, rather indicating a problem with the resolvers than an actual violation of Item 12, which states that such a three-phase transition should not be implemented.

6 Conclusions

This paper reveals that 87.8 % of NSEC3-enabled domains and 47.2 % of TLDs do not follow the best current practice on NSEC3 parameter settings. Our measurements also show a high concentration of non-compliance among a few DNS name server operators and one TLD registry services provider. This indicates that a few organizations could improve the adoption of RFC 9276 to make DNS more robust.

Originally appeared in 2022, it is one year later that the guidance for NSEC3 parameter settings was reappraised when a new critical vulnerability was discovered. Popular resolver implementations promptly reacted to the problem and lowered their limit on additional iterations to 50. Yet, our measurements show that DNSSEC-enabled resolvers in the wild tend to use the limit of 150—the value high enough to enable an efficient DoS attack [24]. Despite the vendor efforts, it is up to DNS administrators to keep their systems up to date. Consequently, recursive resolvers still risk suffering from resource exhaustion attacks.

More generally, the recently discovered CVE and the operational complexity of the hashed authenticated denial of existence raise questions on its usefulness altogether (as evidenced by the mere existence of RFC 9276). We recall that the original NSEC3 RFC aimed at addressing two issues—zone walking and, less known, the high cost of securing unsigned delegations. It was shown that hashing does not prevent deliberate attackers from obtaining the contents of zone files [71, 73]. Moreover, one should take into account the inherent visibility of domain names that can appear in passive DNS feeds or open zone files. Yet, the opt-out flag is the reason why the operators of large zones with many unsigned delegations (such as those of top-level domains) choose NSEC3. Therefore, it remains a reasonable choice among certain DNS operators, even if avoiding zone walking is not their top priority.

One might argue that the CVE impact is less significant due to the low deployment of DNSSEC: despite its existence for almost 20 years, we only found 8.8 % of registered domains to be DNSSEC-enabled. Yet, the goal of our study is to highlight the importance of following best current practices—few iterations in zones and low limits on resolvers—by those actually deploying DNSSEC to reduce the CVE's impact. Hence, we specifically concentrate on authoritative name servers and resolvers deploying DNSSEC, especially those ignoring best current practices.

Future work in the field could concentrate on the following aspects: i) analyze the prevalence of NSEC3 with respect to all the signed domains over time, ii) monitor the maximum additional iteration values enforced by recursive resolvers, and iii) examine NSEC3 parameters used to sign domain names. They will help assess the impact of RFC 9276 and the CVE on the decisions made by DNS administrators.

Acknowledgements

We would like to thank the anonymous reviewers and our shepherd for their valuable feedback on the paper. We also thank RIPE NCC for providing RIPE Atlas credits. This work has been partially supported by the French Ministry of Research projects PERSYVAL Lab under contract ANR-11-LABX-0025-01, DiNS under contract ANR-19-CE25-0009-01, Institut Carnot LSI, and Grenoble Alpes Cybersecurity Institute under contract ANR-15-IDEX-02.

References

[1] Yehuda Afek, Anat Bremler-Barr, and Lior Shafir. 2020. NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 631–648.

[2] Yehuda Afek, Anat Bremler-Barr, and Shani Stajnrod. 2023. NRDelegationAttack: Complexity DDoS attack on DNS Recursive Resolvers. In *32nd USENIX Security*

Symposium (USENIX Security 23). USENIX Association, Anaheim, CA, 3187–3204.
[3] Cathy Almond. 2024. CVE-2023-50868: Preparing an NSEC3 closest encloser proof can exhaust CPU resources. https://kb.isc.org/docs/cve-2023-50868.
[4] Roy Arends, Geoffrey Sisson, David Blacka, and Ben Laurie. 2008. DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. RFC 5155.
[5] Steven M. Bellovin. 1995. Using the Domain Name System for System Breakins. In *5th USENIX UNIX Security Symposium (USENIX Security 95)*. USENIX Association, Salt Lake City, UT, 1–10.
[6] Jonas Bushart and Christian Rossow. 2018. DNS Unchained: Amplified Application-Layer DoS Attacks Against DNS Authoritatives. In *Research in Attacks, Intrusions, and Defenses*. Springer International Publishing, Cham, 139–160.
[7] Cali Dog Security. 2022. Certstream. https://calidog.io.
[8] Christopher Wood, Anbang Wen. 2022. Announcing experimental DDR in 1.1.1.1. https://blog.cloudflare.com/announcing-ddr-support.
[9] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. A Longitudinal, End-to-End View of the DNSSEC Ecosystem. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 1307–1322.
[10] Taejoong Chung, Roland van Rijswijk-Deij, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. Understanding the Role of Registrars in DNSSEC Deployment. In *Proceedings of the 2017 Internet Measurement Conference (IMC '17)*. Association for Computing Machinery, New York, NY, USA, 369–383.
[11] Cloudflare. 2023. Cloudflare 1.1.1.1. https://developers.cloudflare.com/1.1.1.1/.
[12] Cloudflare. 2024. Cloudflare Website and Online Services Terms of Use. https://www.cloudflare.com/website-terms/.
[13] CZ.NIC labs. 2021. Release Notes. https://knot-resolver.readthedocs.io/en/v5.3.1/NEWS.html.
[14] CZ.NIC labs. 2024. Migration. https://www.knot-dns.cz/docs/3.2/html/migration.html.
[15] CZ.NIC labs. 2024. Release Notes. https://knot-resolver.readthedocs.io/en/stable/NEWS.html.
[16] David Dittrich and Erin Kenneally. 2012. *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research*. Technical Report. U.S. Department of Homeland Security. https://catalog.caida.org/paper/2012_menlo_report_actual_formatted.
[17] Domainnameshop. 2024. Domainnameshop. https://domainname.shop/.
[18] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. 2013. ZMap: Fast Internet-wide Scanning and Its Security Applications. In *22nd USENIX Security Symposium (USENIX Security 13)*. USENIX Association, Washington, D.C., 605–620.
[19] Kensuke Fukuda, Shinta Sato, and Takeshi Mitamura. 2013. A Technique for Counting DNSSEC Validators. In *2013 Proceedings IEEE INFOCOM*. IEEE, 80–84.
[20] Oliver Gasser, Quirin Scheitle, Pawel Foremski, Qasim Lone, Maciej Korczyński, Stephen D. Strowes, Luuk Hendriks, and Georg Carle. 2018. Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists. In *Proceedings of the Internet Measurement Conference 2018 (IMC '18)*. Association for Computing Machinery, New York, NY, USA, 364–378.
[21] Sharon Goldberg, Leonid Reyzin, Dimitrios Papadopoulos, and Jan Včelák. 2023. Verifiable Random Functions (VRFs). RFC 9381.
[22] Google Domains. 2024. Google Domains | Official Site. https://domains.google/.
[23] Google Domains. 2024. Use advanced DNSSEC. https://cloud.google.com/dns/docs/dnssec-advanced.
[24] Olivia Gruza, Elias Heftrig, Oliver Jacobsen, Haya Schulmann, Niklas Vogel, and Michael Waidner. 2024. Attacking with Something That Does Not Exist: 'Proof of Non-Existence' Can Exhaust DNS Resolver CPU. In *18th USENIX WOOT Conference on Offensive Technologies (WOOT 24)*. USENIX Association, Philadelphia, PA, 45–57. https://www.usenix.org/conference/woot24/presentation/gruza
[25] Ólafur Guðmundsson and Stephen D Crocker. 2011. Observing DNSSEC Validation in the Wild. *Securing and Trusting Internet Names (SATIN)* (2011).
[26] Wes Hardaker and Viktor Dukhovni. 2022. Guidance for NSEC3 Parameter Settings. RFC 9276.
[27] Elias Heftrig, Haya Schulmann, Niklas Vogel, and Michael Waidner. 2024. The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security*.
[28] Nguyen Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, and Michalis Polychronakis. 2021. How Great is the Great Firewall? Measuring China's DNS Censorship. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 3381–3398. https://www.usenix.org/conference/usenixsecurity21/presentation/hoang
[29] hostnet. 2024. Have a website made. https://www.hostnet.nl.
[30] Hotspoint. 2024. .swiss Domain. https://www.hostpoint.ch/.
[31] IANA. 2024. Root Zone Database. https://www.iana.org/domains/root/db.
[32] ICANN. 2022. Centralized Zone Data Service. https://czds.icann.org.
[33] Internet Systems Consortium. 2021. Release Notes. https://bind9.readthedocs.io/en/v9.16.16/notes.html.
[34] Internet Systems Consortium. 2022. Notes for BIND 9.18.0. https://bind9.readthedocs.io/en/v9.18.0/notes.html.
[35] Internet Systems Consortium. 2023. Release Notes. https://bind9.readthedocs.io/en/v9.19.19/notes.html.
[36] Liz Izhikevich, Gautam Akiwate, Briana Berger, Spencer Drakontaidis, Anna Ascheman, Paul Pearce, David Adrian, and Zakir Durumeric. 2022. ZDNS: a Fast DNS Toolkit for Internet Measurement. In *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22)*. Association for Computing Machinery, New York, NY, USA, 33–43.
[37] Dan Kaminsky. 2008. It's the End of the Cache as We Know It. https://www.slideshare.net/dakami/dmk-bo2-k8.
[38] Marc Kührer, Thomas Hupperich, Jonas Bushart, Christian Rossow, and Thorsten Holz. 2015. Going Wild: Large-Scale Classification of Open DNS Resolvers. In *Proceedings of the 2015 Internet Measurement Conference (IMC '15)*. Association for Computing Machinery, New York, NY, USA, 355–368.
[39] Tho Le, Roland van Rijswijk-Deij, Luca Allodi, and Nicola Zannone. 2018. Economic Incentives on DNSSEC Deployment: Time to Move from Quantity to Quality. In *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 1–9.
[40] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. 2019. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019)*. The Internet Society, Reston, The USA, 1–15.
[41] Wilson Lian, Eric Rescorla, Hovav Shacham, and Stefan Savage. 2013. Measuring the Practical Impact of DNSSEC Deployment. In *22nd USENIX Security Symposium (USENIX Security 13)*. USENIX Association, Washington, D.C., 573–588.
[42] Loopia. 2024. Your own space online for just 9 SEK. https://www.loopia.se/.
[43] Paul Mockapetris. 1987. Domain names - concepts and facilities. RFC 1034.
[44] Paul Mockapetris. 1987. Domain names - implementation and specification. RFC 1035.
[45] NLNet Labs. 2024. Unbound 1.13.2 released. https://www.nlnetlabs.nl/news/2021/Aug/12/unbound-1.13.2-released/.
[46] Yevheniya Nosyk, Maciej Korczyński, and Andrzej Duda. 2023. Extended DNS Errors: Unlocking the Full Potential of DNS Troubleshooting. In *Proceedings of the 2023 ACM Internet Measurement Conference (IMC '23)*. Association for Computing Machinery, New York, NY, USA, 213–221.
[47] Yevheniya Nosyk, Qasim Lone, Yury Zhauniarovich, Carlos H. Gañán, Emile Aben, Giovane C. M. Moura, Samaneh Tajalizadehkhoob, Andrzej Duda, and Maciej Korczyński. 2023. Intercept and Inject: DNS Response Manipulation in the Wild. In *Passive and Active Measurement*. Springer Nature Switzerland, Cham, 461–478.
[48] University of Oregon. 2024. Route Views Project. http://www.routeviews.org/routeviews/.
[49] one.com. 2024. Start your website with one.com. https://www.one.com/en/.
[50] OVHcloud. 2024. Cloud Computing & Web Hosting | OVHcloud Worldwide. https://www.ovhcloud.com/.
[51] Dimitrios Papadopoulos, Duane Wessels, Shumon Huque, Moni Naor, Jan Včelák, Leonid Reyzin, and Sharon Goldberg. 2017. Making NSEC5 Practical for DNSSEC. Cryptology ePrint Archive, Paper 2017/099.
[52] Craig Partridge and Mark Allman. 2016. Ethical considerations in network measurement papers. *Commun. ACM* 59, 10 (sep 2016), 58–64.
[53] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. 2017. Global Measurement of DNS Manipulation. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 307–323. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/pearce
[54] PowerDNS.COM BV. 2022. Changelogs for 4.5.X. https://doc.powerdns.com/recursor/changelog/4.5.html.
[55] PowerDNS.COM BV. 2024. Changelogs for 5.0.X. https://doc.powerdns.com/recursor/changelog/5.0.html.
[56] PowerDNS.COM BV. 2024. Upgrade Notes. https://doc.powerdns.com/authoritative/upgrading.html.
[57] RIPE Atlas. 2020. RIPE Atlas Service Terms and Conditions. https://www.ripe.net/about-us/legal/ripe-atlas-service-terms-and-conditions.
[58] RIPE NCC. 2024. RIPE Atlas. https://atlas.ripe.net/.
[59] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. DNS Security Introduction and Requirements. RFC 4033.
[60] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. Protocol Modifications for the DNS Security Extensions. RFC 4035.
[61] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. Resource Records for the DNS Security Extensions. RFC 4034.
[62] SIE Europe. 2022. Passive DNS Data Sharing. https://www.sie-europe.net.
[63] Technitium. 2024. Technitium DNS Server. https://technitium.com/dns/.
[64] TimeWeb. 2024. Timeweb - Hosting provider and accredited registrar of domains in RU/RF zones. https://timeweb.com/ru/.

[65] TransIP. 2024. High Performance Servers to Power your Infrastructure. https://www.transip.eu/.
[66] Niels L. M. van Adrichem, Norbert Blenn, Antonio Reyes Lua, Xin Wang, Muhammad Wasif, Ficky Fatturrahman, and Fernando A. Kuipers. 2015. A Measurement Study of DNSSEC Misconfigurations. *Secur. Informatics* 4, 1 (2015), 8.
[67] Viktor Dukhovni. 2021. https://twitter.com/VDukhovni/status/1445242037113085956.
[68] Viktor Dukhovni. 2021. NSEC3 parameter selection (BCP: 1 0 0 -). https://lists.dns-oarc.net/pipermail/dns-operations/2021-January/020838.html.
[69] Jan Včelák, Sharon Goldberg, Dimitrios Papadopoulos, Shumon Huque, and David C Lawrence. 2018. *NSEC5, DNSSEC Authenticated Denial of Existence*. Internet-Draft draft-vcelak-nsec5-08. Internet Engineering Task Force. Work in Progress.
[70] Matthäus Wander. 2017. Measurement Survey of Server-Side DNSSEC Adoption. In *2017 Network Traffic Measurement and Analysis Conference (TMA)*. IEEE, 1–9.
[71] Matthäus Wander, Lorenz Schwittmann, Christopher Boelmann, and Torben Weis. 2014. GPU-Based NSEC3 Hash Breaking. In *2014 IEEE 13th International Symposium on Network Computing and Applications*. IEEE Computer Society, Los Alamitos, CA, USA, 137–144.
[72] Matthäus Wander and Torben Weis. 2013. Measuring Occurrence of DNSSEC Validation. In *Passive and Active Measurement*. Springer Berlin Heidelberg, Berlin, Heidelberg, 125–134.
[73] Zheng Wang, Liyuan Xiao, and Rui Wang. 2014. An Efficient DNSSEC Zone Enumeration Algorithm. *Management Innovation and Information Technology* 61 (2014), 459.
[74] Wix.com. 2024. Create a website without limits. https://www.wix.com/.
[75] Suzanne Woolf. 2020. Upcoming DNSSEC changes to PIR delegated Top Level Domains. https://lists.dns-oarc.net/pipermail/org-algorithm-roll/2020-September/000001.html.
[76] Yingdi Yu, Duane Wessels, Matt Larson, and Lixia Zhang. 2013. Check-Repeat: A New Method of Measuring DNSSEC Validating Resolvers. In *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 381–386.

A Ethics and Reproducibility

This paper strictly follows the best practices [16, 18, 52] established by the Internet measurement community. All the subdomains of `rfc9276-in-the-wild.com` have an `A` resource record pointing to a website with a brief explanation of the study and the contact info to opt out of future scans. We carefully configured the `zdns` scanner to limit the number of packets per second sent to `1.1.1.1`. Cloudflare does not set the upper bound on the number of requests coming from a single client [12] and our scan rate was 14.7 K requests per second on average. It is estimated that 600 B requests are seen per day by Cloudflare [8], corresponding to almost 7 M per second. Moreover, given the role of the Cloudflare DNS as a caching resolver, we foresee that a fraction of our queries will be resolved from its internal cache instead of querying authoritative name servers of tested domains. We used the RIPE Atlas Platform, strictly complying with their Terms and Conditions [57] and respecting all the limitations for the number of concurrent measurements and participating probes imposed by the system. The platform itself schedules measurements to balance the load on probes and the whole system in general. All logged IP addresses unrelated to measurement of resolvers were discarded soon after use. We make all the test subdomains available to the community under `rfc9276-in-the-wild.com`.