

Test results

Roy Arends

Shumon Huque

What did we test

- Do legacy resolvers (fail to) ignore:
 - unsolicited
 - signed or unsigned
 - unknown records or authenticated denials of unknown records
 - in a delegation response
 - (such as a new “DELEG” record)
- Do legacy resolvers (fail to) ignore:
 - DS records with an unknown digest
 - unknown flags in DNSKEYs without ignoring the DNSKEY

Parent Zone Setup

legacy.research.icann.org	Baseline standard reference test zone
deleg.research.icann.org	NSEC signed zone containing DELEG
deleg3.research.icann.org	NSEC3 signed zone containing DELEG
delegf.research.icann.org	NSEC signed zone containing DELEG and signal (DNSKEY flag or DS shim)
deleg3f.research.icann.org	NSEC3 signed zone containing DELEG and signal (DNSKEY flag or DS shim)
uns-deleg.research.icann.org	Unsigned zone containing DELEG

Delegation Setup

secure.\$parent	Delegation to a signed zone including a DELEG record. (1)
unsigned.\$parent	Delegation to an unsigned zone including a DELEG record.
no-deleg-secure.\$parent	Delegation to a signed zone without a DELEG record. (2)

1. Not used in unsigned and legacy zone.
2. Not used in unsigned zone.

QNAME	parent signed	child signed	Auth denial	Deleg Signal	Deleg in chain	AD bit expected
txt.no-deleg-secure.legacy	yes	yes	NSEC	no	no	yes
txt.no-deleg-secure.deleg	yes	yes	NSEC	no	no	yes
txt.no-deleg-secure.deleg3	yes	yes	NSEC3	no	no	yes
txt.no-deleg-secure.deleg3f	yes	yes	NSEC3	yes	no	yes
txt.no-deleg-secure.delegf	yes	yes	NSEC	yes	no	yes
txt.secure.deleg	yes	yes	NSEC	no	yes	yes
txt.secure.deleg3	yes	yes	NSEC3	no	yes	yes
txt.secure.deleg3f	yes	yes	NSEC3	yes	yes	yes
txt.secure.delegf	yes	yes	NSEC	yes	yes	yes
txt.unsigned.deleg	yes	no	NSEC	no	yes	no
txt.unsigned.deleg3	yes	no	NSEC3	no	yes	no
txt.unsigned.deleg3f	yes	no	NSEC3	yes	yes	no
txt.unsigned.delegf	yes	no	NSEC	yes	yes	no
txt.unsigned.legacy	yes	no	NSEC	no	no	no
txt.unsigned.unsigned.deleg	no	no	N/A	no	yes	no

Implementations tested

- BIND
 - 9.16.45
 - 9.18.20
 - 9.19.45
- Unbound 1.19.0
- Pdns-recursor
 - 4.7.6
 - 4.9.2
 - 5.0.0rc1
- Knot-resolver 5.7.0

Results

- 120 queries (15 QNAMEs to 8 resolvers).
 - (complete restart of resolver after each query to avoid any state)
- All resulted successfully
 - NOERROR
 - txt record in the answer section
 - AD bit was set where expected.
- Tested resolver implementations have no issue with
 - unsolicited,
 - signed or unsigned,
 - unknown record or authenticated denials of unknown records
 - in a delegation response.
- tested resolver implementations ignore
 - DS records with an unknown digest,
 - unknown flags in DNSKEYs without ignoring the DNSKEY.

Results

- Since then tested with well known public resolvers
 - 8.8.8.8/1.1.1.1/9.9.9.9 etc etc
 - No issues found, same results as the tested resolvers.

Software used for DELEG testing

- Shumon Huque's adns-server.py:
 - https://github.com/shuque/adns_server