draft-ietf-dnsop-nsec3-iterations

Wes Hardaker and Viktor Dukhovni

November 11, 2021

NSEC Iterations Value Capping

Primary point of the current draft

- Use NSEC if you can
- NSEC3 iterations recommendation: 0
- NSEC3 salt: only use one if you're going to change it
- Validating resolvers:

			Action
0	–	100	Validate
101	–	500	SHOULD Insecure
501	+		MAY SERVFAIL

Deployment figures today

- recent NSEC iteration deployment stats as of Nov 4:

Stat	Value	Was
Total NSEC3 measured zones	12,460,057	11,488,499
Fraction <= 0	0.07935	
Fraction <= 10	0.92455	
Fraction <= 20	0.99183	
Fraction <= 100	0.99979	0.99942
Fraction <= 150	0.99840	
Fraction <= 500	0.**99999**655	0.99999634

[Thank you to Viktor for his measurements]

Remaining outstanding question

What lower iterations limit to use?

draft		
	previous draft	150
	Current draft	100
validator		
	four current	150
	two promised	100
DNSOP participants	favor	0

Potential consensus?

Validators

SHOULD	iterations > 0	insecure/ignore
MAY	iterations $= 1$	insecure/ignore
MUST	iterations > 100	insecure/ignore
MAY	iterations > 500	SERVFAIL

Zone Owners

SHOULD	use	iterations $= 0$
MUST	use	iterations $<= 100$