nsec3.2

Wes Hardaker and Viktor Dukhovni

November 12, 2021

Let's try this again

Recent lessons learned

A. We want Zone publishers to move to iterations = 0

Recent lessons learned

A. We want Zone publishers to move to iterations = 0

B. We want validators to start enforcing lower counts

Recent lessons learned

A. We want Zone publishers to move to iterations = 0

B. We want validators to start enforcing lower counts

C. SERVFAIL is better than insecure

Recent lessons learned

A. We want Zone publishers to move to iterations = 0

B. We want validators to start enforcing lower counts

C. SERVFAIL is better than insecure

D. Do all of this at a reasonable deployment rate

Recent lessons learned

A. We want Zone publishers to move to iterations = 0

B. We want validators to start enforcing lower counts

C. SERVFAIL is better than insecure

D. Do all of this at a reasonable deployment rate

E. [Reasonable deployment rate is likely large]

How to get from NULL to A. . . .

A. We want Zone publishers to move to iterations = 0

How to get from NULL to A. . . .

A. We want Zone publishers to move to iterations = 0

> *2 Recommendation for zone publishers*
>
> *2.3 Iterations*
>
> *[. . .]*
>
> *NSEC mitigates this concern, and if NSEC3 must be used then an iterations count of 0 SHOULD be used.*
>
> *– Paul Hoffman proposal [with edits]*

How to get from A to B/D...

B. We want validators to start enforcing lower counts

D. Do all of this at a reasonable deployment rate

How to get from A to B/D...

B. We want validators to start enforcing lower counts

D. Do all of this at a reasonable deployment rate

> *4 Recommendation for validating resolvers*
>
> *[...]*
>
> *As of November 2021, setting an upper limit of 100 iterations for treating a zone as insecure is interoperable without significant problems, but at the same time still enables CPU-exhausting DoS attacks.*
>
> *For this reason validating software vendors are encouraged to continue evaluating NSEC3 iteration count deployments and lower their default and acceptable limits over time.*
>
> *– Petr Špaček proposal [with edits]*

How to get from A to B/D to C

C. SERVFAIL is better than insecure

How to get from A to B/D to C

C. SERVFAIL is better than insecure

> *4 Recommendation for validating resolvers*
> *[. . .]*
> *Similarly, because treating NSEC3 with a high iterations count as insecure leaves zones subject to attack, validating software vendors are further encouraged to lower their default and acceptable limits for returning SERVFAIL for large iteration count values. As of November 2021, setting an upper limit of 500 iterations above which SERVFAIL should be interoperable without significant problems.*
> *– Wes' proposal*

A proposed appendix

Iterations	QPS [% of 0 iterations QPS]
0	100 %
10	89 %
20	82 %
50	64 %
100	47 %
150	38 %

[data is courtesy of Petr Špaček]